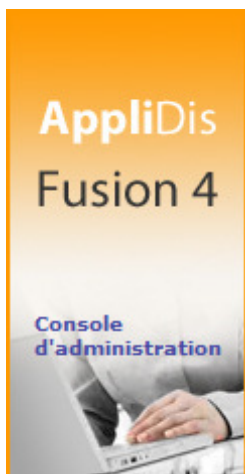




Administration manual





Copyright © Systancia 2010 – All rights reserved. Systancia and AppliDis are trademarks of Systancia.

The information provided in this document is by way of information only, and does not therefore constitute any kind of commitment for Systancia. The information contained herein may be amended by Systancia at any time without notice.

This document and the AppliDis software are covered by a user license. This is not a transfer of ownership. The user is required to accept the user license agreement at installation time. Users who do not wish to accept this user license should not install the AppliDis software. Under the terms of the user license, no reproduction or unauthorised use of all or part of the AppliDis software is permitted. This includes this document: no part of this documentation may be reproduced or transmitted in any form by any means whatsoever for any use other than the personal use of the purchaser, except with the express written agreement of Systancia.

This document is intended for experienced users who have a basic understanding of the Microsoft Windows operating system. Systancia shall not be held liable for any handling errors in the use of the AppliDis software. The use of this product is the sole responsibility of the user.

Trademarks of other companies: all other trademarks, product names and company names referred to in this document are mentioned for explanatory purposes and belong to their respective holders. More specifically, Microsoft, Windows, Windows 2000, Windows 2003 and Windows 2008 Server are trademarks of Microsoft Corporation in the United States and in other countries.

Systancia
Actipolis 3
3, rue Paul Henri Spaak
68390 Sausheim
France

Telephone: (+33) 3 89 33 58 20
Fax: (+33) 3 89 33 58 21
Web: <http://www.Systancia.com>
email: commercial@systancia.com

AppliDis Fusion documentation version 4.0 SP1 – v1.02

Table of contents

TABLE OF CONTENTS	3
TABLE OF ILLUSTRATIONS	9
1 APPLIDIS FUSION 4 IN BRIEF	13
1.1 DELIVER APPLICATIONS AND DESKTOPS AS A SERVICE	13
1.2 DEPLOY "USER EXPERIENCE 2.0"	13
1.3 SIMPLIFY DAY-TO-DAY ADMINISTRATION TASKS	13
2 THE VARIOUS VERSIONS OF APPLIDIS FUSION 4	14
2.1 APPLIDIS FUSION	14
2.2 APPLIDIS FUSION SSO	14
3 LICENSING MODES FOR APPLIDIS FUSION 4	15
3.1 APPLIDIS FUSION 4 TRIAL VERSION LICENSE	15
3.2 APPLIDIS FUSION LICENSE	15
3.3 APPLIDIS FUSION SSO LICENSE	15
4 THE VARIOUS APPLIDIS FUSION 4 INTERFACES	16
4.1 ADMINISTRATION INTERFACE - APPLIDIS ADMINISTRATION	16
4.2 APPLICATION ACCESS INTERFACE - APPLIDIS CLIENT	16
5 THE VARIOUS APPLIDIS SERVER ROLES	23
5.1 INTRODUCTION	23
6 APPLIDIS HIGH AVAILABILITY	24
6.1 REDUNDANCY OF APPLIDIS APPLICATION HOST SERVERS AND WINDOWS DESKTOP SERVERS	24
6.2 REDUNDANCY OF VIRTUAL MACHINE HOST SERVERS	24
6.3 REDUNDANCY OF ADMINISTRATION AND CONNECTION BROKER SERVERS	24
6.4 REDUNDANCY OF APPLIDIS DATABASES	24
6.5 REDUNDANCY OF THE APPLIDIS GATEWAY	25
7 CLIENT REQUIREMENTS	26
7.1 CONFIGURATION OF THE WORKSTATION	26
7.2 CONFIGURATION OF A THIN CLIENT	26
7.3 SPECIAL THIN CLIENT CASES	27
8 REQUIREMENTS AND SERVER PREPARATION	28
8.1 INTRODUCTION	28
8.2 REQUIREMENTS FOR AN APPLIDIS SERVER	28
8.3 INSTALLATION OF REDUNDANT APPLIDIS ADMINISTRATION AND CONNECTION BROKER SERVERS	34

8.4 REQUIREMENTS FOR THE DATABASES	34
MICROSOFT INTERNET INFORMATION SERVER CONFIGURATION	36
8.5 CONFIGURATION OF MICROSOFT TERMINAL SERVICES OR REMOTE DESKTOP	39
8.6 FIXED IP ADDRESS	46
8.7 INSTALLATION OF APPLIDIS ON A DOMAIN CONTROLLER	47
8.7.1 ON 2000/2003 SERVERS:	47
8.7.2 ON 2008/2008R2 SERVERS	48
9 DEPLOYMENT SCENARIOS	48
9.1 SIMPLE CONFIGURATION: ONE SERVER AND SEVERAL CLIENTS	48
9.2 SEVERAL SERVERS WITH LOAD BALANCING	50
9.3 REDUNDANCY OF THE ADMINISTRATION SERVERS AND APPLICATION LOAD BALANCING	51
9.4 CONFIGURATION WITH A ROUTER FOR REMOTE LOCATIONS	52
10 INSTALLATION	53
10.1 PROCEDURE	53
10.2 INSTALLATION OF THE APPLIDIS ADMINISTRATION SERVER	53
11 AFTER INSTALLATION	58
11.1 START MENU	58
11.2 POST-INSTALLATION CONFIGURATION SETTINGS	58
11.3 LOCATION OF DIRECTORIES AND FILES	59
11.4 UNINSTALLING APPLIDIS	60
12 NAVIGATING IN THE ADMINISTRATION CONSOLE	61
13 USING APPLIDIS IN A FEW STEPS	63
14 ACCESSING THE APPLIDIS ADMINISTRATION	65
15 USER MANAGEMENT	66
15.1 OPERATING PRINCIPLE	66
15.2 USER MANAGEMENT BY SYNCHRONIZATION	66
15.3 THE SYNCHRONIZED MODE OF USER MANAGEMENT IS ACTIVATED IF THE "DYNAMIC USER MANAGEMENT" OPTION IS UNCHECKED (SEE PAGE: 184, "ACTIVE DIRECTORY	66
15.4 DYNAMIC USER MANAGEMENT	72
15.5 COMMON USER FUNCTIONS	78
15.6 REDIRECTION OPTIONS FOR LOCAL DISKS, PRINTERS AND PERMANENT DESKTOP OPTION	79
16 SERVER INSTALLATION AND MANAGEMENT	81
16.1 INTRODUCTION	81
16.2 ADMINISTRATION AND CONNECTION BROKER SERVER	82
16.3 WEB USER PORTAL SERVER	82
16.4 APPLIDIS GATEWAY	83
16.5 ACTIVATING THE HTTP GATEWAY	87
16.6 CONFIGURING THE SETTINGS OF THE CLIENT ZONES USING THE HTTP GATEWAY	88
16.7 CREATING AND REMOVING SERVER GROUPS	90
16.8 APPLICATIONS ON APPLICATION SERVERS	91
16.9 MONITORING AND MAINTENANCE OF SERVERS	92
17 MANAGEMENT OF CLIENT DESKTOPS	94
17.1 PLACING ICONS ON THE USER'S DESKTOP	94

17.2	APPLICATION SECURITY	94
17.3	MANAGEMENT OF FILE EXTENSIONS	94
17.4	CONNECTIONS	95
18	MYAPPS CATALOGUE	97
18.1	CONFIGURATION	97
18.2	APPLICATION ACCESS REQUEST	97
18.3	MANAGEMENT OF PUBLIC APPLICATIONS	98
18.4	MANAGEMENT OF ACCESS TO THE CATALOGUE	98
19	APPLICATION MANAGEMENT	98
19.1	LIST OF APPLICATIONS	98
19.2	PRINCIPLE OF APPLICATION REFERENCING	98
19.3	ADVANCED REFERENCING OF APPLICATIONS	100
19.4	LIST OF AVAILABLE SERVERS TO AN APPLICATION	102
19.5	MANUAL REFERENCING OF AN APPLICATION	102
19.6	ADD AN APPLICATION TO THE MYAPPS CATALOGUE	104
19.7	ADVANCED PROPERTIES OF AN APPLICATION	104
19.8	ADDING / ACTIVATING / DEACTIVATING A LOCATION FOR AN APPLICATION	105
19.9	REMOVING AN APPLICATION OR REMOVING AN APPLICATION LOCATION	107
19.10	CREATING AND REMOVING APPLICATION GROUPS	108
19.11	ASSIGNING RELATIONSHIPS BETWEEN APPLICATIONS AND APPLICATION GROUPS	109
19.12	APPLICATION PRIORITY LEVELS	111
19.13	NORMAL MODE OR APPLICATION MODE FOR APPLICATIONS	112
19.14	SELECTING THE APPLICATION ICON	113
20	DESKTOP MANAGEMENT	113
20.1	LIST OF DESKTOPS	113
20.2	LIST OF CLONES	118
21	CONTRACT MANAGEMENT	123
21.1	CONTRACT PRINCIPLE	123
21.2	ADDING A CONTRACT	124
21.3	REMOVING A CONTRACT	125
21.4	MODIFYING A CONTRACT	126
22	MANAGEMENT OF PRIVILEGES	126
22.1	MANAGEMENT OF SERVER PRIVILEGES	127
22.2	MANAGEMENT OF APPLICATION PRIVILEGES	128
22.3	MANAGEMENT OF OPTION PRIVILEGES	128
23	USING THE DASHBOARD	129
23.1	PRINCIPLE OF THE DASHBOARD	129
23.2	VIEWING THE INFORMATION	129
23.3	DEACTIVATE A SERVER	131
23.4	INTERACTING WITH CURRENT APPLICATIONS	132
23.5	INTERACTING WITH CURRENT DESKTOPS	133
24	ALARM MONITORING AND REPORTING	134
24.1	VIEWING THE EVENT LOGS	134
24.2	VIEWING THE RESOURCES	136

24.3	VIEWING MICROSOFT TSE SESSIONS	137
24.4	ALARM SETTINGS	137
24.5	DEFINITION OF THE MONITORING AUTHORITY	139
24.6	DEFINITION OF INFORMATION TRANSMISSION METHODS	140
25	VIEWING THE STATISTICS	156
25.1	INSTALLING THE MACROMEDIA SHOCKWAVE PLUG-IN	156
25.2	STATISTICS SUMMARIES	156
25.3	STATISTICS BY SERVER	157
25.4	STATISTICS BY APPLICATION	160
25.5	STATISTICS BY USER	163
25.6	STATISTICS BY DESKTOP	165
25.7	SEARCH IN THE STATISTICS	168
26	PRINTING	169
26.1	PRINT FORMAT	169
26.2	UNIVERSAL PRINTER CONFIGURATION	169
26.3	PRINT OPTIONS	169
26.4	PARAMETER SETTING OF THE TRANSFER RATES ACCORDING TO CLIENT ZONES	170
26.5	DEDICATED UNIVERSAL PRINTER PER NAMED SESSION	171
26.6	PRINTING WITH THE UNIVERSAL PRINTER	173
26.7	NETWORK PRINTER FILTERING	173
27	SCANNING	175
27.1	GENERIC PERIPHERALS	175
27.2	ACTIVATING SCANNING	175
27.3	PARAMETER SETTING OF TRANSFER RATES ACCORDING TO CLIENT ZONES	175
28	APPLIDIS DELEGATED ADMINISTRATION	176
28.1	ADDING A DELEGATED ADMINISTRATION GROUP/OU	176
28.2	CONFIGURING ZONES	177
28.3	CONFIGURING ROLES	177
28.4	REMOVING A GROUP/OU	178
28.5	GENERAL REMARKS ABOUT THE MANAGEMENT OF DELEGATED ADMINISTRATION PRIVILEGES MODULE:	179
29	APPLIDIS CONFIGURATION	180
29.1	GENERAL INFORMATION	180
29.2	APPLIDIS LICENSE	180
29.3	ACTIVE DIRECTORY	181
29.4	GENERAL OPTIONS	184
29.5	LOAD BALANCING	187
SECONDARY DATABASES		190
29.6	CREATION OF BACKUP DATABASES	190
29.7	SCRIPTS	192
29.8	LANGUAGES	192
30	DATABASE MAINTENANCE	193
30.1	REQUIREMENTS	193
30.2	MANUAL DATA CLEANSING	193
30.2.1	RESETTING DATA USAGE STATISTICS	193

30.2.2	RESET DATA USAGE STATISTICS AND IMPORTED USERS	193
30.2.3	RESET DATA USAGE STATISTICS, IMPORTED USERS AND CREATED CONTRACTS.	193
30.2.4	RESET DATA USAGE STATISTICS, IMPORTED USERS, CREATED CONTRACTS AND IMPORTED USER GROUPS.	193
30.2.5	RESET CREATED CONTRACTS AND USER ACCESS TOKENS IN USE.	193
30.3	AUTOMATED DATA CLEANING	193
30.4	RESTORING THE MAIN DATABASE	194
31	ADVANCED CONFIGURATION AND OPERATION OF APPLIDIS FUSION	196
1	APPLIDIS TOOLBOX	196
2	SAVING INFORMATION (BACKUP)	196
2.1	BACKING UP DATABASES	197
2.2	RESTORING DATABASES	198
2.3	BACKING UP FILES	199
2.4	RESTORING FILES	199
2.5	SAVING REGISTRY KEYS	200
3	DATABASE MANAGEMENT	200
3.1	RESETTING THE DATA OF THE BACKUP DATABASES	201
3.2	RESTARTING A DATABASE SERVER	201
4	RESTARTING THE SERVERS	202
4.1	RESTARTING AN ADMINISTRATION SERVER	202
4.2	SEQUENCE FOR RESTARTING A SERVER WHICH IS BOTH ADMIN AND SQL AT THE SAME TIME	202
4.3	RESTARTING AN APPLICATION SERVER	203
5	MAINTENANCE OF APPLIDIS SERVERS	203
5.1	REPLACING AN APPLICATION SERVER	203
5.2	CHANGING THE IP ADDRESS OF AN APPLICATION SERVER	204
5.3	RENAMING AN APPLICATION SERVER	204
5.4	RENAMING AN ADMINISTRATION SERVER	204
6	APPLICATIONS ISOLÉES	205
	PRÉSENTATION DE L'ISOLATION SYSTÈME	205
	PRINCIPE	205
	INTERET	205
	REFERENCEMENT D'UNE APPLICATION ISOLEE DANS APPLIDIS	205
	PRE-REQUIS	205
	REFERENCEMENT D'UNE MACHINE VIRTUELLE CLIENT	206
	REFERENCEMENT D'UNE APPLICATION SUR UN SYSTEME ISOLE	208
	CREATION D'UN CONTRAT SUR UNE APPLICATION ISOLEE	208
7	APPLIDIS VDI	208
7.1	APPLIDIS VDI SERVICE RIGHTS	208
7.2	MICROSOFT INTERNET EXPLORER CERTIFICATE VALIDITY	210
	CONFIGURATION OF A VIRTUAL MACHINE	211
7.3	CREATION OF A VIRTUAL MACHINE REFERENCE	211

7.4	CONFIGURATION OF A VIRTUAL MACHINE REFERENCE	211
7.5	APPLIDIS VDI CONFIGURATION	223
7.6	APPLIDIS VDI ACTIVATION	224
7.7	HOW TO REFERENCE THE VIRTUAL MACHINES?	225
7.8	CONFIGURATION OF A MACHINE REFERENCE	231
7.9	CREATION OF A DESKTOP POOLS	231
7.10	USER GROUP CONFIGURATION	238
7.11	CONTRACT CONFIGURATION	241
7.12	CLIENT PORTAL	243
1	OVERVIEW OF THE MICROSOFT TERMINAL SERVER	244
2	MICROSOFT TERMINAL SERVER USER LICENSES	245
2.1	INTRODUCTION	245
2.2	LICENSE OPERATING PROCESS	245
2.3	INSTALLATION AND CONFIGURATION	245
2.4	MICROSOFT INTERNET CONNECTOR LICENSE	247
3	PRINTING WITH TERMINAL SERVER	247
3.1	REDIRECTING LOCAL PRINTERS	247
3.2	REDIRECTING NETWORK PRINTERS	247
3.3	PRINTERS NOT RECOGNIZED BY THE SERVER	248
3.4	APPLIDIS TOOLS FOR PRINTING	248
3.4.1	PRINTER MANAGER	249
3.4.2	PRINT QUEUE MANAGER	249

Table of illustrations

Figure 1 - Access page for the administration console	16
Figure 2 - Acceptance of execution of the AppliDis client.....	18
Figure 3 - Gnome desktop with AppliDis applications.....	19
Figure 4 - Window disconnection button	19
Figure 5 - AppliDis in desktop mode.....	20
Figure 6 - AppliDis virtual desktop (locked down desktop).....	21
Figure 7 - BureauVirtuel.exe (Remote desktop AppliDis 'locked down' connection).....	27
Figure 8 - Installation of Internet Information Server on Windows 2000 Server.....	36
Figure 9 - Installation of Internet Information Server on Windows 2003 Server.....	37
Figure 10 - List of roles in the Windows 2008 server manager	37
Figure 11 - Adding a role on Microsoft Windows 2008 Server.....	37
Figure 12 - Visibility of Internet Information Services (IIS) roles on Windows 2008 Server.....	38
Figure 13 - Selection of IIS services to be installed on Windows 2008 server.....	38
Figure 14 - Installation of Microsoft Terminal Server services on Windows 2000 Server.....	40
Figure 15 - Configuration of the operating mode of Microsoft Terminal Server services.....	40
Figure 16 - Installation of Microsoft Terminal Server services on Windows 2003 Server.....	41
Figure 17 - List of roles in the Microsoft Windows 2008 server manager	42
Figure 18 - Adding a role on Microsoft Windows 2008 Server.....	42
Figure 19 - Configuration of Terminal Server services on Microsoft Windows 2008 Server.....	43
Figure 20 - Remote App settings on Microsoft Windows 2008 Server.....	44
Figure 21 - List of roles in the Microsoft Windows 2008 R2 server manager	44
Figure 22 - Adding a role on Microsoft Windows 2008 R2 Server.....	45
Figure 23 - Configuration of Remote Desktop services on Microsoft Windows 2008 R2 Server.....	45
Figure 24 - Remote App settings on Microsoft Windows 2008 R2 Server.....	46
Figure 25 - Internet Protocol (TCP/IP) Properties.....	47
Figure 26 - Configuration with one Application Server and one Administration Server.....	49
Figure 27 - Configuration with several application servers.....	50
Figure 28 - Configuration with several administration servers.....	51
Figure 29 - Configuration with several administration servers, access by router and Gateway	52
Figure 30 - Command Prompt change user.....	53
Figure 31 - Run as administrator.....	54
Figure 32 - Windows 2008 Install Application on Microsoft Terminal Server.....	54
Figure 33 - Selection of database type	55
Figure 34 - Configuration of a Microsoft SQL database	56
Figure 35 - Configuration of an Oracle 10g database	57
Figure 36 - Homepage of the AppliDis administration site.....	61
Figure 37 - AppliDis Administration Console (User search page)	78
Figure 38 - "Save as" window showing access to local disks under Windows 2000.....	80
Figure 39 - Gateway and load balancing	83
Figure 40 - Gateway and protection of application servers	84
Figure 41 - Configuration of the Gateway access URL.....	88
Figure 42 - IP range of clients not using the HTTP Gateway.....	89
Figure 43 - Connections to server group.....	95
Figure 44 - Removing a server from a group	96

Figure 45 - Desktop list	114
Figure 46 - Desktop creation (step 1).....	115
Figure 47 - New desktop creation, localization (step 2).....	116
Figure 48 - New desktop creation (Machine setup, step 3)	116
Figure 49 - New desktop creation (Summary, step 4)	117
Figure 50 - Desktop creation (percentage %).....	117
Figure 51 - Desktop properties (General information).....	118
Figure 52 - Clone list	119
Figure 53 - New clone to be associated	120
Figure 54 - Clone information & properties.....	121
Figure 55 - Example of general view of the Dashboard (application servers load balancing)	129
Figure 56 - Confirmation box.....	130
Figure 57 - Dashboard – applications in progress	130
Figure 58 - Confirmation box.....	131
Figure 59 - Dashboard (running desktops in progress).....	131
Figure 60 - Search for security events on AppliDis servers.....	135
Figure 61 - Display of system information for all servers	135
Figure 62 - Viewing disks resources	136
Figure 63 - Viewing memory resources	136
Figure 64 - Viewing CPU resources	137
Figure 65 - End of alarm parameter setting	139
Figure 66 - Monitoring authority parameter setting	140
Figure 67 - Configuration of alarm recipients	141
Figure 68 - Descriptive diagram of SNMP protocol.....	142
Figure 69 - Configuration of SNMP services.....	153
Figure 70 - SNMP service startup configuration.....	154
Figure 71 - Configuration of the SNMP manager.....	155
Figure 72 - Example of display of the use of an application over a year.	161
Figure 73 - Example of display of the use distribution of the various users.	164
Figure 74 - Example of display of the use of an desktop over a year.....	166
Figure 75 - Parameter setting of transfer rates according to IP zone	170
Figure 76 - Options for automatically mounting a universal printer	172
Figure 77 - Printer selection box on the server	173
Figure 78 - Activating network printer access filtering.....	174
Figure 79 - Activating scanning	175
Figure 80 - Parameter setting of transfer rates according to IP zone	176
Figure 81 - Administration groups.....	176
Figure 82 - List of zones.....	177
Figure 83 - Multi-domain authentication (AppliDis User Web portal).....	181
Figure 84 - Active Directory information	182
Figure 85 - Active Directory connection settings.....	183
Figure 86 - Configuration of AppliDis general options	187
Figure 87 - Configuration of backup databases on the AppliDis Administration console.....	190
Figure 88 - Creation of an SQL backup database on the AppliDis Administration console	191
Figure 89 - Creation of a backup database using the internal engine (AppliDis Administration console)	191
Figure 90 – Database cleansing menu	194
Figure 91 – Notification database in safe mode	195

Figure 92 – Switching back to the main database	196
Figure 93 - Liste des serveurs AppliDis	206
Figure 94 - Choix de la machine d'isolation	206
Figure 95 - Installation du rôle serveur d'applications sur la machine virtuelle.....	207
Figure 96 - Fin de l'installation du rôle serveur d'applications	207
Figure 97 - La machine isolée est un serveur d'applications.....	208
Figure 98 - ADISVDIService Properties (Local Computer)	209
Figure 99 - Security (Internet Options).....	210
Figure 100 - Turning off Windows Firewall	212
Figure 101 - Windows Firewall/Internet Connection Sharing Service (ICS).....	213
Figure 102 - Allow log on through Terminal Services (GPO)	214
Figure 103 - Computer System Properties (Remote Desktop).....	215
Figure 104 - Add... users to the Remote Desktop Users	216
Figure 105 - Remote Registry Properties (Local Computer).....	217
Figure 106 - Remote Procedure Call (RPC) Service	218
Figure 107 - Windows Management Instrumentation Properties Service	219
Figure 108 - WMI Control (Local) Properties	220
Figure 109 - Security (Permissions for Admins).....	221
Figure 110 - COM+ Event System Properties Service	222
Figure 111 - VMWare Menu (Install/Upgrade VMWare Tools).....	223
Figure 112 - Devices with Removable Storage.....	223
Figure 113 Activate VDI Service (AppliDis Management Console)	224
Figure 114 - Add virtual machines host (AppliDis Management Console)	225
Figure 115 - VDI Connection Configuration (AppliDis Management Console).....	226
Figure 116 - Referencing virtual machines on host... (Management Console)	227
Figure 117 - Virtual machines on host SrvVcenter (AppliDis Management Console).....	228
Figure 118 - Virtual Machine Host in the Server list (AppliDis Management Console).....	229
Figure 119 - Available Virtual machines (AppliDis Management Console)	230
Figure 120 - Desktop list (AppliDis Management Console)	231
Figure 121 - New Desktop (AppliDis Management Console).....	232
Figure 122 - Localization, New Desktops (AppliDis Management Console).....	233
Figure 123 - Host & Reference virtual machine (AppliDis Management Console).....	233
Figure 124 - Reference virtual machine (AppliDis Management Console)	234
Figure 125 - Machine setup (AppliDis Management Console).....	235
Figure 126 - Desktops list summary (AppliDis Management Console).....	236
Figure 127 - Desktop installation process (AppliDis Management Console)	236
Figure 128 - Clones list Menu (AppliDis Management Console).....	237
Figure 129 - User groups menu (AppliDis Management Console)	238
Figure 130 - Add groups by selected OU (AppliDis Management Console).....	238
Figure 131 - User groups (AppliDis Management Console).....	239
Figure 132 - User group properties (AppliDis Management Console).....	239
Figure 133 - Options from the User groups menu (AppliDis Management Console)	240
Figure 134 - New Contract (AppliDis Management Console).....	241
Figure 135 - Associate a user group to a Desktop (AppliDis Management Console).....	242
Figure 136 - Your desktops client portal menu (AppliDis client)	243
Figure 137 - Example of access to a printer in two modes (network and local).....	247



Introduction

The AppliDis administration module provides a simple way of managing an entire network of AppliDis servers, the users, applications and desktops associated with AppliDis.

It provides a fast and user-friendly way of displaying the applications and/or Desktops in use and the users that are connected. AppliDis provides the administrator with a tool which allows to manage remotely the number of simultaneous instances of applications. This tool is based on the concept of application contracts, which enables us to define in particular the term of the contract and the maximum number of licenses granted for this application (which corresponds to the maximum number of applications that can be executed simultaneously).

Thanks to statistics and the other information provided (such as feedback and user controlled alerts) regarding all the servers of the network, the administrator can analyze performance and take proactive measures to adapt the AppliDis system to the actual needs of the company while offering a very high level of availability and performance.

AppliDis also offers a universal printer that optimizes and channels print flows. AppliDis also includes an HTTP or HTTPS access module for remote access through your firewalls and proxy servers without compromising your security.

The advanced version of AppliDis also offers very high operational availability through the redundancy of all components and a Virtual IP protection device in addition to intelligent load balancing.



Introduction to AppliDis Fusion 4

SP1

AppliDis Fusion 4 is a complete solution for the virtualisation of user environments. It manages and virtualises all Windows applications and workstations from the company's data centre. AppliDis Fusion 4 provides all the necessary functions for total control over your user environments and a significant improvement in service quality.

With AppliDis Fusion 4, you can deliver all your applications to users on demand, regardless of their physical location or method of connection (office network, roaming WiFi, roaming 3G, home network).

1 AppliDis Fusion 4 in brief

1.1 Deliver applications and desktops as a service

With AppliDis Fusion 4, it is possible to deliver applications and desktops as a service. Applications and virtual workstations are managed and deployed via a Web console.

Based on the RDP protocol included with Windows RDS (formerly known as Windows TS), and compatible with all industry hypervisors (Hyper-V, ESX, ESXi, Virtualcenter, etc.), AppliDis Fusion 4 is able to virtualise all your applications and desktops.

Virtual desktops can operate under the Windows XP, Vista and Seven operating systems (VDI technology) via AppliDis Connexion Broker, or work as a Windows RDS / Terminal Server desktop (Windows 2000 to Windows 2008 R2).

At the user level, access is possible via a web browser, an AppliDis Desktop client (a client which automatically displays published icons on the desktop or on the Start menu), or through a distributed desktop on a thin client.

1.2 Deploy "User Experience 2.0"

With AppliDis Fusion 4, the user experience in a virtualised environment is an enriched and interactive one. Multimedia content such as video streams, Flash animations, DirectX and two-way sound are supported by default. External peripherals are automatically recognised immediately upon connection to the user's desktop.

Thanks to the new AppliDis MyApps™ virtualised applications catalogue included in AppliDis Fusion 4, users are able to choose which applications they want and think they will need for their everyday work. Access to these applications is then either approved or denied by the administrator.

1.3 Simplify day-to-day administration tasks

With AppliDis Fusion 4, the day-to-day administration and running of virtual environments becomes extremely simple. A single, friendly admin control panel in Web format provides control

over all the functions available in AppliDis Fusion 4: management of servers, applications, publication contracts, access privileges and the creation and management of virtual machines.

AppliDis Fusion 4 provides you with an entire toolbox of technical resources. In this way, AppliDis ToolBox delivers a certain number of system tools such as a virtualisation tool for registry keys (for each application), a tool for virtualising directories, hostnames, etc. All tools are catalogued and detailed under the AppliDis administration console.

2 The various versions of AppliDis Fusion 4

2.1 AppliDis Fusion

This version contains all the features that companies require to optimize the total cost of running an information system.

Combining several modules it fulfils the needs of all SME-SMI companies with a network of 10 computers or major accounts with a large computer network, including one or more server farms and more specialized performance requirements.

- ✓ Enables them to centralize all their applications in current use and to make them accessible over the Intranet and Extranet.
- ✓ Smart Load Balancing Module This module carries out a multidimensional statistical analysis of the information system so as to choose the most suitable server in real time.
- ✓ Ensures a very high level of continuity of service through the redundancy of all AppliDis components (Administration, Database, Applications and Gateway) protected by an integrated virtual IP address device.

2.2 AppliDis Fusion SSO

A version offering all the advantages of the Fusion version as well as a Single Sign-On (SSO) module which controls and manages strong authentication functions and the Single Sign-On application.

This module addresses security issues such as:

- deletion of passwords recorded in clear text
- support for all application types
- increased password complexity and automatic periodic password changing
- improved access controls
- traceability: actions and events auditing

In this way, this version strongly reduces the cost of ownership of IT infrastructure by reducing support calls and increasing user productivity.

Furthermore, AppliDis SSO is compatible the strong authentication systems such as smart cards, biometrics, one-time passwords (OTP). The authentication mechanism allows the following:

- Authentication through physical devices
- Access to alternative means of connection
- Direct access to a self service – connection mode which allows a user to connect without its usual authentication process using a question/answer type system.
- Compatibility with OTP solutions such as SecurID RSA, Vasco Digipass, Safeword secure computing first access.
- Management of physical devices and simplified rollout of cards/tokens.

- Centralised management of physical devices (registration in Directory, management of blank, lost or recovered cards).
- Creation of black lists.

This component is natively integrated in AppliDis Fusion 4. The installation beforehand of the SSOX solution in the centralised environment is a prerequisite.

The items added in the AppliDis console are as follow:

- **Users.** Search and administration of users.
- **Profils.** Recording of SSO information.
- **Q&A.** In case the password is forgotten, this allows users to connect through a series of questions and answers.
- **Admin Configuration.** Configuration of the Administration part.
- **Configuration.** Directory configuration.
- **SC.** Management of peripherals (smart card).
- **Customisation.** Definition of users who can have access to the tool.

3 Licensing Modes for AppliDis Fusion 4

The various versions of AppliDis Fusion 4 require different kinds of user licenses . Your AppliDis partner will supply you with one of the following user licenses in accordance with your choice, represented by a user code (e.g.: *8ysxGagIWj2UYgIdPU/w5OwqBcB8NMgRZ B2rD9Y*).

3.1 AppliDis Fusion 4 trial version license

If you are using an evaluation version of AppliDis Fusion 4, you will have full use of AppliDis Fusion 4 with all its features for 31 days, as a default. If you wish to extend the duration of the trial, the following options are available:

- A period of use,
- A maximum number of Application servers.
- A limited number of simultaneous users.

3.2 AppliDis Fusion license

With an AppliDis Fusion license you will have all the load balancing functions of AppliDis Fusion and you can install as many application servers as you wish.

The AppliDis Fusion license system is based on the number of authorised concurrent users.

Your AppliDis partner will provide you with a serial number defining the number of authorized simultaneous users. If you wish to increase this number, all you need to do is to update your license with your partner; no reinstallation is necessary.

3.3 AppliDis Fusion SSO license

With an AppliDis Fusion SSO license, you have access to all the features of the AppliDis SSO version, including the Single Sign-On function. You may install as many application servers as you wish.

The AppliDis Fusion SSO license system is based on the number of authorised concurrent users.

Your AppliDis partner will provide you with a serial number defining the number of authorized simultaneous users. If you wish to increase this number, all you need to do is to update your license with your partner; no reinstallation is necessary.

4 The Various AppliDis Fusion 4 Interfaces

In order to make AppliDis as easy to use as possible, its main interfaces are based on a Web browser.

The main kinds of interfaces are described below.

4.1 Administration interface - AppliDis Administration

The administration component is based on a Web interface, which will enable you to manage the entire AppliDis application easily from any workstation in your network. All administrative actions are carried out exclusively by this administration interface, which is based on the use of the Internet Information Server (IIS) service and Active Server Pages technology.

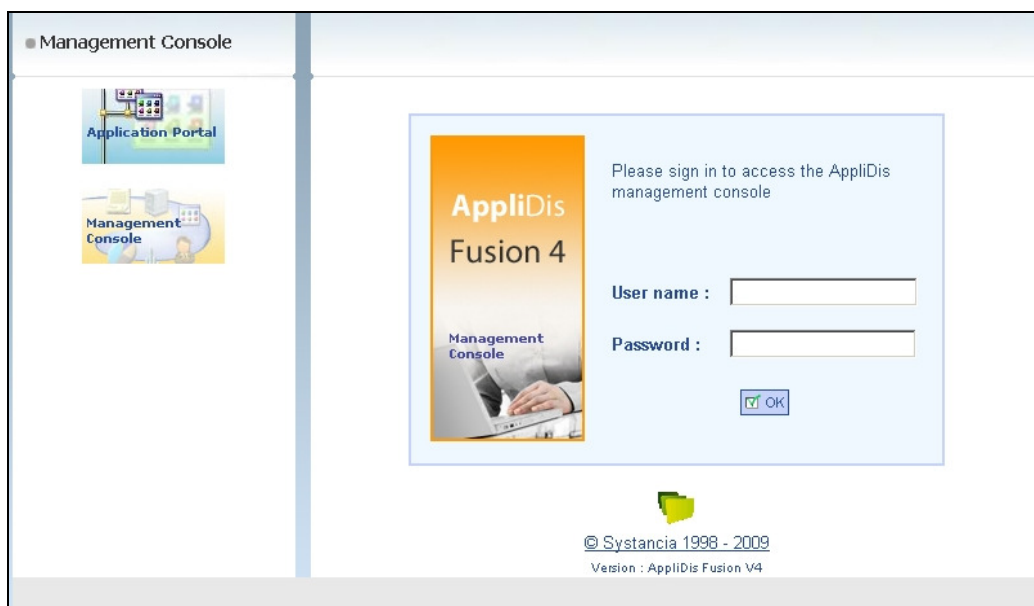


Figure 1 - Access page for the administration console

Microsoft Internet Explorer is recommended for the management of AppliDis.

4.2 Application access interface - AppliDis Client

AppliDis Fusion 4 offers access to applications in a highly transparent way to the user via a variety of methods.

One of these methods is identical to launching an application installed on the workstation using shortcuts from the desktop or in the user's Start menu.

In addition, users can customise their applications list to filter out all but the most common applications which they access the most.

AppliDis MyApps

The AppliDis MyApps catalogue allows users to request access to one or more applications placed by the administrator in the AppliDis MyApps catalogue. It is then up to the administrator to approve or deny the user's request. If the user's request is approved, the application will appear along with the other applications to which he/she already has access privileges.

Furthermore, a comments and scoring area is available for applications, enabling users to review applications to assist other users in choosing which new applications to use.

Access methods

There are various ways to access applications from AppliDis. The table below provides a summary of these ways, which will then be described in more detail.

Access mode	Description	Type of access
"AppliDis Web"	Access from a Web browser (Internet Explorer or Firefox)	Via a browser, the user has access to all his applications from a secure URL. The applications will be launched in the same environment as the browser.
"AppliDis Desktop"	Access from the desktop of a Windows operating system	The user has additional icons and shortcuts on the standard desktop of his Windows operating system. These icons and shortcuts can be used to launch applications in the operating system environment.
"AppliDis RDP Boot"	Full desktop access from a thin client or a Linux operating system	The user has access to a full virtualized desktop. The user will have access to his applications in this secure and personalized desktop. This desktop will provide traditional operation from a thin client or a Linux operating system.

Type of client	Compatibility	Access to AppliDis	Access to functions
Web	Windows (for Firefox with JRE 1.5.8) Linux (with JRE 1.5.8) Mac XPE CE	AppliDis Web	Virtualised applications Virtual desktops
Windows	Windows XPE CE	AppliDis Desktop	Virtualised applications Virtual desktops
Thin Client		AppliDis RDP Boot	Virtual desktops

In addition, users have access to their virtualised applications from every virtual desktop.

AppliDis Secondary Access

"Command line - AppliDis Launcher"	Access to applications via command line	The administrator can personalize the access to applications for Windows users from programs or scripts by using the utility command line, AppliDis Launcher.
"TSE session mode"	TSE sessions will be shown on the Dashboard.	Full RDP connection handling the automatic resumption of sessions and the resumption of open sessions.

Via a Web portal from a Microsoft Internet Explorer browser

This access mode is known as "application portal".

The application portal is the simplest way for all your users to access the applications. Once the privileges have been set via the administration console, users will be able to execute their usual applications from this portal, or access sessions they have disconnected from. The application portal can be accessed from the Internet Explorer and Firefox browser families. There is also the option of managing the graphical styles of the AppliDis site via a CSS file.

Via a Web portal from a Mozilla Firefox browser

This access mode is also known as "application portal"; it is only the choice of the browser that is different from the preceding mode.

AppliDis has a Java client running under Windows or Linux, from a simple Mozilla Firefox browser (3.1 and above) and the Java plug-in (JRE 1.6). The AppliDis Client is executed in the form of a Java Applet (Signed JAR archive). When using it for the first time, you are required to accept the signed JAR.

When you work with the AppliDis Java client, the application disconnection function can be accessed by clicking on the button displayed as a circle in the window of your application (see Figure 4 - Window disconnection button).



Figure 2 - Acceptance of execution of the AppliDis client

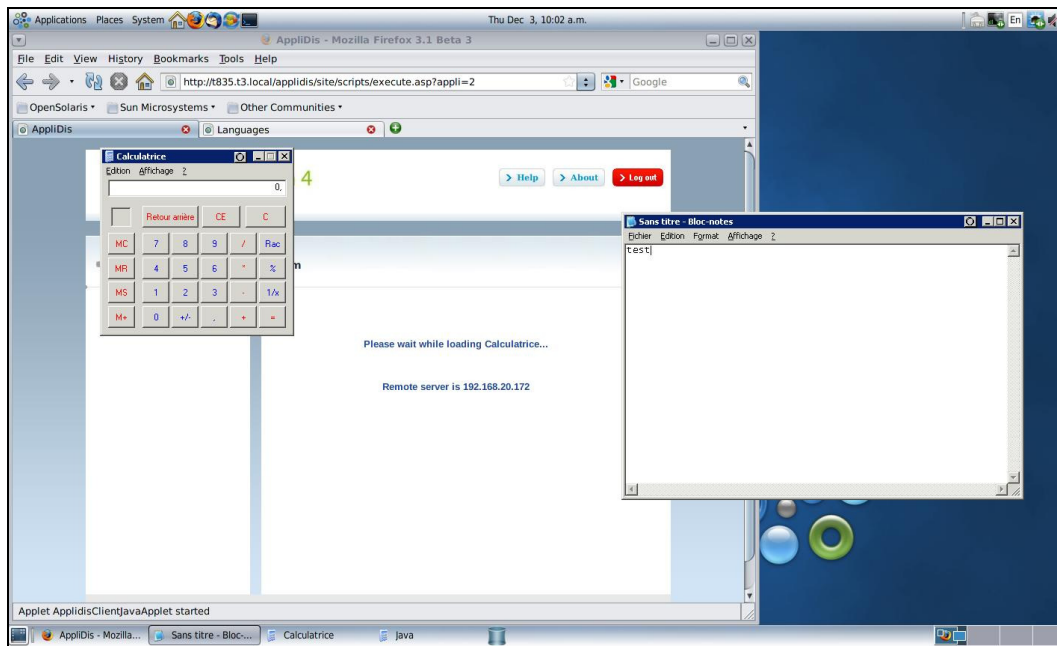


Figure 3 - Gnome desktop with AppliDis applications



Figure 4 - Window disconnection button

Java client limitations:

The Java client has some limitations:

- Printer redirection (Microsoft Terminal Server).

These limitations can be worked around using various integration techniques, for example by implementing Samba for the Linux client.

Via the desktop of a Microsoft Windows operating system

Desktop mode is an extra feature to the application portal for users who wish to bridge the gap between the use of an application via AppliDis and the use of an application in the traditional way.

AppliDis will be available in the Windows taskbar in the form of a red icon (disconnected) or a green icon (connected). Desktop mode has the following features:

- Execute AppliDis applications from the Windows Desktop. The applications are available in the form of desktop icons.
- Execute AppliDis applications from the Windows start menu. The applications are placed in an AppliDis file in the start menu.
- Execute applications from application files (for example a .doc document file) and load files that are on the user's workstation.
- Resume disconnected applications (i.e. applications that are open on the server but from which the user has disconnected) from a menu (right click) on the AppliDis icon on the Windows taskbar. This operation can be performed automatically when the user connects to AppliDis (see: **"Smart Connection" technology** p.186)



Figure 5 - AppliDis in desktop mode

Via a virtual desktop from a light client or a Linux operating system

The virtual desktop provides a user-friendly AppliDis work interface from any kind of thin client. This interface also allows clients based on operating systems other than Windows to access applications published by AppliDis, in particular Linux with RDESKTOP.

Virtual desktop mode appears as a desktop in which:

- Published applications are placed in the start menu and/or published directly on the desktop (this option can be activated by the system administrator via the controls of the administration console of the product). Applications are automatically and dynamically placed in the start menu or directly on the desktop (if this option is activated).
- Users have the option of placing shortcuts to files/applications/directories directly on the desktop.

This virtual desktop also features an option for the administrator to protect his environment by placing restrictions on the launching of executables or certain types of files (see the section on security management on the client workstation).

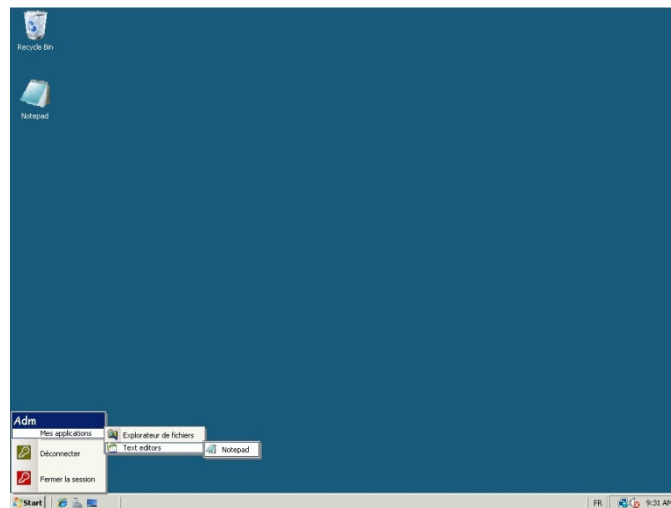


Figure 6 - AppliDis virtual desktop (locked down desktop)

With this access mode you can also publish the Windows file explorer which enables you to browse the file systems (the client's or the network's).

Via the Microsoft TSE session marker from a light client or a Linux operating system

This mode gives access to a full TSE desktop. Opening a session makes the most of load balancing and the resumption of disconnected and/or active sessions (see: **"Smart Connection" technology**, p.186).

This mode is used in the same way as the virtual desktop. For the virtual desktop, the program "bureauvirtuel.exe" is started in the RDP connection. For TSE session mode, the program "AdisBureau.exe" is started.

Example: A user has a TSE desktop open on 1 server. He is disconnected following an interruption in the network service.

When he is reconnected on another server, he will see the applications that were open at the time of the disconnection in this new session.

Via a command line - AppliDis Launcher

With the AppliDis Launcher utility, an application published by AppliDis can be launched in a simple and very flexible way. AppliDis Launcher works as a program that is called from the command line. It can thus be called up by a compiled executable or script.

The required arguments are:

- The name of the published application to be executed: this is the name of the application which can be seen in the administration console; names are case-sensitive (see page: 101 **"Renaming an application"**).
- Optional: the user name followed by the password. If these parameters are omitted, the Desktop client connection information is used. Alternatively, an AppliDis authentication window is displayed.

Example:

```
"C:\Systancia\Applidis\ApplidisLauncher.exe" -a "Word" -u "user01" -p "password"
```

5 The various AppliDis server roles

5.1 Introduction

This section describes in detail the various roles available at AppliDis infrastructure server level.

Role	Description
AppliDis Administration Server and Connection Broker	This centralises all useful information and also assigns users to various "Application Host Servers and Windows Desktops" or "Virtual Machine Host Servers" (if there is load balancing). AppliDis administrators and users communicate with the Administration Server through their Internet Explorer browser.
Web Users Portal server	The Web Users Portal server makes it possible to set a server as a specialist portal server. Attacks on the platform can be limited in this way.
Gateway server	The Gateway service is a tool integrated into AppliDis which makes it possible to increase the security of the Application Servers when it is accessed from the Internet. It also has a load balancing function which is intended for thin clients and other platforms, (rdesktop for Linux for example). Load balancing does not require a gateway for "workstation" type clients. A gateway is a feature which is placed between AppliDis clients and the Application Server to which they are connected. It makes it possible to redirect a request to open an AppliDis session to the most suitable Application Server (load balancing), based on information given by the AppliDis Administration Server. In redundancy mode of the Administration servers protected by virtual IP, it is advisable to deploy the Gateway on all the Administration servers.
HTTP Gateway Server	AppliDis integrates a gateway functionality "HTTP Gateway" (not to be mistaken with the standard AppliDis Gateway) which allows the AppliDis client to operate from any kind of Internet access. This gateway uses the HTTP/HTTPS protocol and thus does not require specific router or firewall configuration in the client infrastructure networks. Furthermore, it is compatible with any proxy that may be used. By setting IP range parameters, clients connecting through the Gateway can be distinguished from clients that connect directly (RDP).
Applications Host and Windows Desktops server	The applications are installed, and will be run, on this TSE server. The servers can be homogeneous (all installed in the same way) or heterogeneous (some servers only have certain applications).
Virtual Machines Host server	This server produces virtual OS images from reference virtual images which are cloned to give users the virtual desktop they wish to use.

6 AppliDis High Availability

6.1 Redundancy of AppliDis Application Host servers and Windows Desktop servers

AppliDis intelligent load balancing continuously scans the availability of the Application Host Servers and Windows Desktops. In the event of a failure of a server in your farm, the AppliDis load balancing feature will automatically exclude any applications or Windows Desktops from starting up on this server. Once the server is operational again, it can once again be accessed for all new requests to start applications or Windows Desktops.

Furthermore, please note that a system to protect against the "Black-Hole" effect is in place in the AppliDis load balancing engine. This makes it possible to artificially lower the grade of a server receiving a certain number of simultaneous connections. What may happen is that when the system is under load and a new unit is added, the new unit may be repeatedly selected by the load balancer, taking into account the imbalance of the calculated load. The server grade that is lowered in this way is valid until the server information is updated. Terminal Servers do not in fact readily support very fast session opening requests.

6.2 Redundancy of Virtual Machine Host servers

AppliDis intelligent load balancing continuously scans the availability of the Virtual Machine Host Servers. In the event of a sever failure in your farm, the AppliDis Fusion 4 load balancing feature will automatically exclude any virtual machines from starting up on this Host. Once the server is operational again, it can once again be accessed for all new requests to start virtual machines.

Scores are allocated to the various hosts according to 3 criteria's:

- the dynamic resources for each host server
- The number of available virtual machines in the pool
- The number of virtual machines already running on the host.

In addition, there is a 'virtual machine predictive launch' mechanism, based on user experience (same day of the week and same hour of the day), which allows a certain number of virtual machines to be running before even being requested by users, to ensure that users do not waste time launching virtual machines; in this way, optimised times are achieved for virtual machine start-up from 'sleep' mode..

6.3 Redundancy of Administration and Connection Broker servers

Administration and Connection Broker servers also profit from the redundancy feature. A floating or virtual IP mechanism based on IP Aliasing enables the Administration department to ensure maximum continuity of service even in the event of the breakdown of a server. AppliDis configuration data are placed on an SQL Server 2000 or 2005 database, which is also redundant.

6.4 Redundancy of AppliDis databases

AppliDis Administration and Connection Broker servers are based on a common database. As protection against any failure of this database, up to five backup databases can be configured from the AppliDis Administration console.

6.5 Redundancy of the AppliDis gateway

The AppliDis Gateway can be deployed on any server of your AppliDis server farm. However, in order to benefit from the Virtual IP protection of the Administration servers, they need to be deployed specifically on these servers. Thus, if one Gateway is unavailable, the other one will implicitly take over. This device also ensures maximum continuity of service for an AppliDis farm located behind Firewall.



Preparing for AppliDis Fusion 4 deployment

Before installing AppliDis, the servers have to be checked to ensure they are correctly configured in order to accommodate AppliDis.

7 Client requirements

7.1 Configuration of the workstation

AppliDis can be used on any client workstation running a version of Windows (from Windows 95 to Windows 7).

Microsoft Internet Explorer software must be version 5.0 or above to use AppliDis.

However, an operating system of the Windows 95, Windows 98 or NT type requires the following elements to be installed:

- "Win95 Service Pack 1 Update" available from:
http://www.microsoft.com/windows95/downloads/contents/WURecommended/S_WUServicePacks/W95SvcPack1/Default.asp
- "Microsoft Windows Sockets Update" available from:
http://www.microsoft.com/windows95/downloads/contents/wuadmintools/s_wunetworkingtools/w95sockets2/default.asp

Microsoft Internet Explorer version 5.5 or higher in order to use AppliDis Client in desktop mode (the standard version 5.0 is sufficient for the use of AppliDis Client in application portal mode).

When the AppliDis Administration Server is configured in authenticated mode (IIS default configuration), it is advisable to add the address of this server to the list of "Local Intranet" sites of your Internet Explorer browser.

For Windows XP Service Pack 2 or 3 users and Windows Vista or Windows 7 users, the URL of the AppliDis server must also be added to the list of "Local Intranet" sites.

7.2 Configuration of a thin client

AppliDis works with any type of thin client implementing the RDP protocol, regardless of the operating system used (Linux, CE, CE .NET, XPe, etc.).

The use of thin clients with AppliDis requires the following configuration settings on these devices:

- Application Server or Gateway Server address, if several AppliDis servers are deployed. If you set up redundancy of the Administration servers with IP protection and if you deploy the AppliDis Gateway on these two servers, the virtual IP address or DNS record should be inserted in place of the server name.
- Service port (by default 3389 or 5300 if the AppliDis Gateway is used).
- Session opening program: **BureauVirtuel.exe** to use the extended AppliDis virtual desktop.

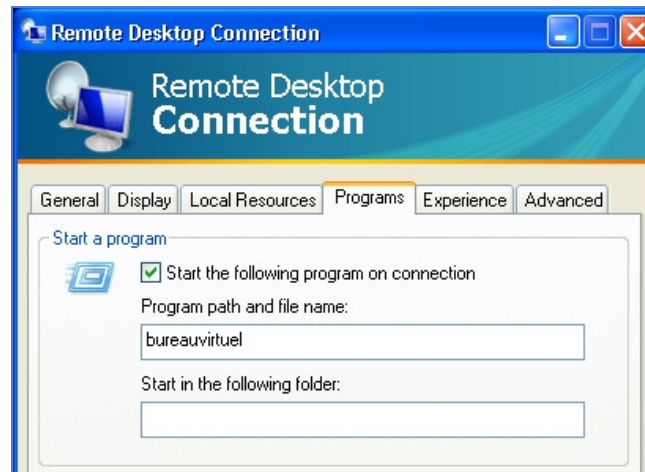


Figure 7 - BureauVirtuel.exe (Remote desktop AppliDis 'locked down' connection)

Note: Some types of thin clients do not allow setting of the service port. As a result, this remains at 3389. Contact your hardware retailer's support service to change this configuration setting. Some manufacturers provide add-ons to carry out this operation.

7.3 Special thin client cases

Some thin clients natively load the Windows XPe operating system (XP Embedded). Depending on the XPe components installed by the manufacturer (generally hard-wired into a ROM), AppliDis can be run directly from the integrated browser. Thus, the user connects to AppliDis through the portal and starts up his application by clicking on the icon. In this case, AppliDis works in the same way as a fat workstation operating under Windows XP.

8 Requirements and server preparation

8.1 Introduction

The aim of this section is to draw up the list of components required by AppliDis, which must be installed on the server or servers before installing AppliDis, and to describe the install process.

8.2 Requirements for an AppliDis server

This section concentrates on the following items:

- Administration and Connection Broker Server
- Web User Portal server
- Gateway Server and HTTP Gateway Server,
- Applications Host and Windows Desktops server
- Virtual Machine Host server.

Definitions

An "AppliDis Administration service" or "AppliDis Administration and Connection Broker Server" is installed from a CD-ROM.

The "AppliDis Administration and Connection Broker Server" can be installed on several servers to provide maximum continuity of service for AppliDis. It has to be installed from the CD-ROM each time, in the same target path (e.g. C:\Program Files\Systancia\). If several Administration and Connection Broker servers are installed, each server is configured to be able to access the database. The Virtual IP mechanism (see page 85 "

Setting the virtual IP address") defines a single access point for all your servers, even in the event of a breakdown. The Application Servers must also be located in the same IP network to benefit from Virtual IP protection.

To run the AppliDis setup, you need to be physically in front of the server or to be in Microsoft TSE console mode.

A "**Presentation Portal service**" or "**Web User Portal server**" is automatically installed on an "AppliDis Administration and Connection Broker Server" and can be deployed from the management console. Since its installation is controlled by the latter, the CD-ROM is no longer needed. This installation can be carried out on one or more devices in order to obtain one or more "AppliDis Web User Portal Servers". This role can be installed on an Application Host and Windows Desktop Server and/or gateway/HTTP gateway server.

This client web portal can be put in a demilitarised zone (DMZ) as a complement to the AppliDis "HTTP Gateway". Thus enabling the applications published by this portal to be available without any other AppliDis components being directly accessible.

It should be noted that a standalone presentation server does not benefit from the hot redundancy mechanism via the virtual IP address which is reserved for the Administration Servers (administration and presentation services on the same server).

If applications are being used and the presentation portal is unavailable, these applications remain active. However, users will not be able to launch any additional applications.

A router with LSNAT functionality can be used to set up this kind of redundancy. This is identical to virtual IP but is managed by an active device.

An **"AppliDis Gateway service"** or **"AppliDis Gateway Server"** is installed after an "AppliDis Administration and Connection Broker Server" has been installed. Since its installation is controlled by the latter, the CD-ROM is no longer needed. This installation can be carried out on one or more devices in order to obtain one or more "AppliDis Gateway Servers". Lastly, it can be installed on one single device that already has an "AppliDis Administration and Connection Broker Server". In this case, this device will have to meet the requirements for an "AppliDis Administration and Connection Broker Server" and the requirements for an "AppliDis Gateway Server" at the same time. This kind of server has multiple roles: firstly, it will provide load balancing for thin clients. It will then improve site security by acting as a "compulsory intermediary" for client workstations wishing to connect to the Application Host and Windows Desktop Servers.

An **"AppliDis http Gateway service"** or **"AppliDis http Gateway Server"** is installed after an "AppliDis Administration and Connection Broker Server" has been installed. Since its installation is controlled by the latter, the CD-ROM is no longer needed. This installation can be carried out on one or more devices in order to obtain one or more "AppliDis HTTP Gateway Servers". Lastly, it can be installed on one single device that already has an "AppliDis Administration and Connection Broker Server". In this case, this device will have to meet the requirements for an "AppliDis Administration and Connection Broker Server" and the requirements for an "AppliDis http Gateway Server" at the same time. The role of such a server is to propose and manage the encapsulation of RDP packets in HTTP or HTTPS packets. It will then improve site security by acting as a "compulsory intermediary" for client workstations wishing to connect to the Application Host and Windows Desktop Servers. These relay servers are particularly useful to facilitate the passage of firewall servers or other proxy servers for external access. Indeed, the service of encapsulating RDP packets in HTTP/HTTPS mode means that additional ports do not have to be opened towards the outside. A high level of network security is thus maintained

Note: When you change the default installation path of the AppliDis Administration and Connection Broker Server, you must make sure that this path will be appropriate for all the other server components. In particular if you install AppliDis on the D:\ disc, all the servers deploying AppliDis components will use this D:\ disc as their install path.

An **"AppliDis Application service"** or **"AppliDis Application Host and Windows Desktop Server"** is deployed after an "AppliDis Administration and Connection Broker Server" has been installed. Since its installation is controlled by the latter, the CD-ROM is no longer needed. This installation can be carried out on one or more devices in order to obtain one or more "AppliDis Application Host and Windows Desktop Servers". Lastly, it can be installed on one single device that already has an "Administration and Connection Broker Server". In this case, this device will have to meet the requirements for an "AppliDis Administration and Connection Broker Server" and the requirements for an "AppliDis Application Host and Windows Desktop Server" at the same time. The Application Host and Windows Desktop servers then allow applications and the Windows desktop to run and be presented to the user.

An **"AppliDis Virtual Machines service"** or **"AppliDis Virtual Machines Host Server"** is deployed after an "Administration and Connection Broker Server" has been installed. Since its installation is controlled by the latter, a CD-ROM is no longer needed. This installation can be carried out on one or more devices in order to obtain one or more "AppliDis Virtual Machines Host Servers". The "AppliDis Virtual Machine Host servers" then enable the virtual machines to be hosted, run, and presented to the user.

General requirements

The Microsoft Terminal Services license manager must be installed and operational in your domain. The licenses or "TSE CALs " must also be activated on your clients. A DNS server must also be present and correctly configured in your environment.

The AppliDis Servers' NetBIOS hostnames can only contain alphanumerical characters (A-Z, a-z, 0-9) and the character "-". All the other characters are not supported by AppliDis.

Requirements of an "AppliDis Administration and Connection Broker Server"

It must have a server version of the one of the following Windows operating systems:

- Microsoft Windows 2000 Server (Service pack 4) in a standard or advanced version
- Microsoft Windows 2003 Server (Standard, Enterprise, R2) with or without Service Pack x86 ou x64.
- Microsoft Windows 2008 Server (Standard, Enterprise, R2) x86 ou x64.

The "AppliDis Administration and Connection Broker Server" must have the following tool installed and correctly configured:

- Microsoft Internet Information Server (IIS), see "
- Requirements for installation of an **Oracle 10g database**
- Oracle 10g Server
- Oracle 10g Client (10.2.0.3)
- **Oracle user** account with the privileges "Resource", "Connect" and "Unlimited TableSpace" on the database server.

- Microsoft Internet Information Server Configuration", p. 35.

In Administration and Connection Broker server redundancy mode, the following points must be satisfied in order to use the Virtual IP.

- The Administration and Connection Broker servers must be located in the same LAN (same IP network).
- "DHCP Client" services must be stopped (start-up of the manual service). If you stop the **DHCP Client** service, your computer will no longer receive dynamic IP addresses and automatic dynamic DNS updates will no longer be recorded on the DNS server. In addition, if this service is deactivated, any service which explicitly depends on it will fail.
- You have to set the name of the servers manually in the DNS and in your WINS server, if you have one. Of course, the device's static address must be specified.
-

Note: In redundancy mode, you can install an Administration and Connection Broker Server in another LAN, in which case this server must be excluded from the list of devices eligible for virtual IP.

Make sure you have assigned a static IP address to your server. If the DHCP Client service is deactivated, your server will no longer be visible on the network.

Requirements for an "AppliDis Web User Portal server"

It must have a server version of the one of the following Windows operating systems:

- Microsoft Windows 2000 Server (Service pack 4) in a standard or advanced version
- Microsoft Windows 2003 Server (Standard, Enterprise, R2) with or without Service Pack x86 ou x64.
- Microsoft Windows 2008 Server (Standard, Enterprise, R2) x86 ou x64.

The "Web Users Portal Server" must have the following tool installed and correctly configured:

- Microsoft Internet Information Server (IIS), see "
- Requirements for installation of an **Oracle 10g database**
- Oracle 10g Server
- Oracle 10g Client (10.2.0.3)
- **Oracle user** account with the privileges "Resource", "Connect" and "Unlimited TableSpace" on the database server.

- Microsoft Internet Information Server Configuration", p. 35.

Requirements of an "AppliDis Gateway Server"

It must have a server version of one of the following Windows operating systems:

- Microsoft Windows 2000 Server (Service pack 4) in a standard or advanced version.
- Microsoft Windows 2003 Server (Standard, Enterprise, R2) with or without Service Pack x86 or x64.
- Microsoft Windows 2008 Server (Standard, Enterprise, R2) x86 or x64.

These services can also be deployed on Windows 2000 Pro or XP Pro workstations.

Requirements of an "AppliDis http Gateway Server"

It must have a server version of the one of the following Windows operating systems:

- Microsoft Windows 2000 Server (Service pack 4) in a standard or advanced version
- Microsoft Windows 2003 Server (Standard, Enterprise, R2) with or without Service Pack x86 or x64.
- Microsoft Windows 2008 Server (Standard, Enterprise, R2) x86 or x64.

The "AppliDis HTTP Gateway Server" must have the following tools installed and correctly configured:

- Microsoft Internet Information Server (IIS), see "
- Requirements for installation of an **Oracle 10g database**
- Oracle 10g Server
- Oracle 10g Client (10.2.0.3)
- **Oracle user** account with the privileges "Resource", "Connect" and "Unlimited TableSpace" on the database server.

- Microsoft Internet Information Server Configuration", page 35.

This service can also be placed on a Web Users Portal server. This would make it possible to unify the external access points (Web Users Portal server and http Gateway Server).

Requirements for an "AppliDis Applications Host and Windows Desktop server"

It must have a server version of the one of the following Windows operating systems:

- Microsoft Windows 2000 Server (Service pack 4) in a standard or advanced version
- Microsoft Windows 2003 Server (Standard, Enterprise, R2) with or without Service Pack x86 or x64.
- Microsoft Windows 2008 Server (Standard, Enterprise, R2) x86 or x64.

The "AppliDis Application Host and Windows Desktop Server" must have the following tools installed and correctly configured:

- Microsoft Internet Information Server (IIS), see "
- Requirements for installation of an **Oracle 10g database**
- Oracle 10g Server
- Oracle 10g Client (10.2.0.3)
- **Oracle user** account with the privileges "Resource", "Connect" and "Unlimited TableSpace" on the database server.

- Microsoft Internet Information Server Configuration", page 35.
- Microsoft Services Terminal Server (TSE)

Requirements for a "Virtual Machine Host Server"

It must have a version of one of the following virtualisation systems:

- VMware ESX and ESXi version 3.5 Update 3
- VMware ESXi 3.5 Update 4 and ESXi 4, depending on the license used (30-day trial license OK, licensed by vCenter OK, **Warning! The free ESXi version 4 license does not work with AppliDis Fusion 4**)
- VMware Virtual center version 2.5
- Microsoft Hyper-V.

8.3 Installation of redundant AppliDis Administration and Connection Broker servers

AppliDis Administration and Connection Broker servers can be installed in redundant mode in your environment for maximum availability of your applications. The first Administration and Connection Broker Server installed will be known as the Main Administration Server; subsequent ones will be known as Secondary Administration Servers. If only one AppliDis Administration and Connection Broker Server is installed, it will of course be the main server. All the servers are linked to the same single database. The requirements for the database will depend on the choice you make. The options will be set out later on.

Main Administration server

When the main server is installed, AppliDis Installer will create a database in accordance with the information provided (SQL 2000 or SQL 2005 Server).

Secondary Administration servers

When the secondary AppliDis servers are installed, the Installer will link the secondary server to the database (SQL 2000 or SQL 2005 Server).

8.4 Requirements for the databases

The requirements set out below depend on the type of database you decide to use. They are valid for the database required for installation but also for any backup databases you configure later on.

Requirements for installation of a Microsoft SQL Server 2000 or MSDE database

The following elements are required in order to use a Microsoft **SQL Server 2000 SP4** database:

- Microsoft SQL Server 2000 SP4 installed on a server in your domain and configured in **mixed** mode. It must also accept network connections.
- **SQL user** account with **SA** privileges on the database server (System Administrator).

Requirements for installation of a Microsoft SQL 2005 SERVER database

- SQL 2005 Express or SQL 2005 Server.
- **SQL user** account with **SA** privileges on the database server (System Administrator).

Requirements for installation of a Microsoft SQL 2008 SERVER database

- SQL 2008 Express or SQL 2002 Server.
- **SQL user** account with **SA** privileges on the database server (System Administrator).

Note: AppliDis does not install any SQL Server components in your environment. However, the database instance and the various config settings are entirely automated.

In SQL 2005 and SQL 2008 Server mode, AppliDis uses ODBC compatible Microsoft SQL 2000 Server drivers (present on Windows 2000, 2003 and 2008 Server), so there is no need to install any special components on your servers (for example, the SQL 2005 Server Native Client).

Requirements for installation of an Oracle 10g database

- Oracle 10g Server
- Oracle 10g Client (10.2.0.3)
- **Oracle user** account with the privileges "Resource", "Connect" and "Unlimited TableSpace" on the database server.

Microsoft Internet Information Server Configuration

Internet Information Server is Microsoft's Intranet/Internet server software. It is available in installations of Windows 2000, 2003 and 2008 Server. Internet Information Server must be installed on the device accommodating the AppliDis administrator and the AppliDis Application Servers.

Installing Microsoft Internet Information Server on Windows 2000 Server

1. In the Start menu, click on Settings, then on Control Panel.
2. Select Add/Remove Programs, then Add/Remove Windows Components.
3. Tick the Internet Services (IIS) box (**Erreur ! Source du renvoi introuvable.** on Windows 2000 Server). In the Details section, required information is: Internet Information services (IIS) Snap-in, Common Files, World Wide Web server.
4. Click on OK.
5. Click on Next to finish installation.

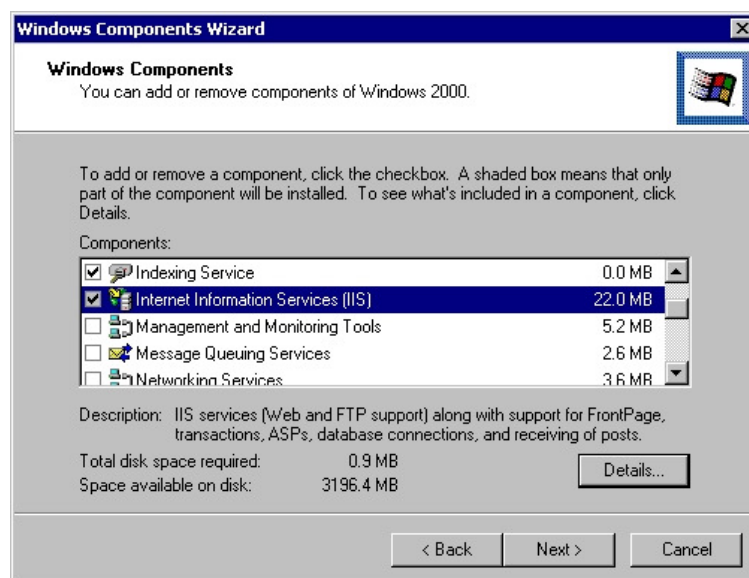


Figure 8 - Installation of Internet Information Server on Windows 2000 Server

Installing Internet Information Server on Microsoft Windows 2003 Server

1. In the Start menu, then the Control Panel; select Add/Remove Programs, then Add or Remove Windows Components.
2. In the window which opens, called the Windows Components Assistant, select the Application Server line. The essential elements in the Details section are: IIS Service, Activate COM+ network access.
3. Click on Next to finish installation.

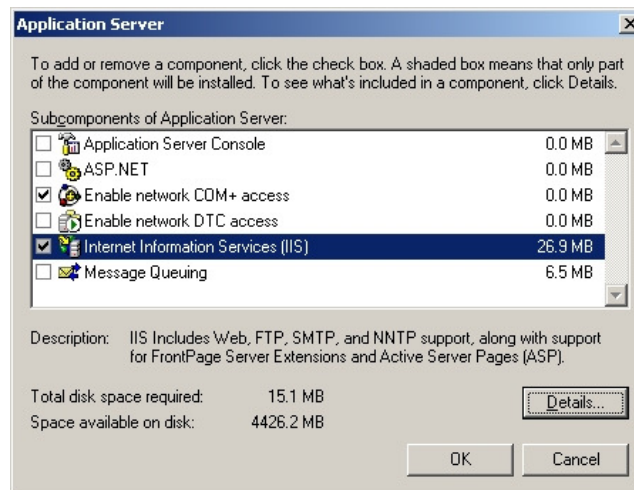


Figure 9 - Installation of Internet Information Server on Windows 2003 Server

Installing Internet Information Server on Windows 2008 Server or R2

In the **Server Manager** window, check if the **Web server (IIS)** role is installed.

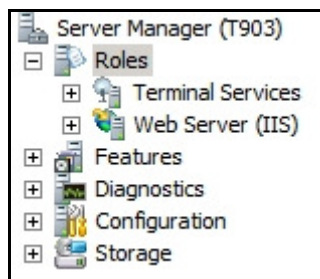


Figure 10 - List of roles in the Windows 2008 server manager

This role can be installed from the "**Roles Summary**" sub-menu in the **Server Manager** screen.

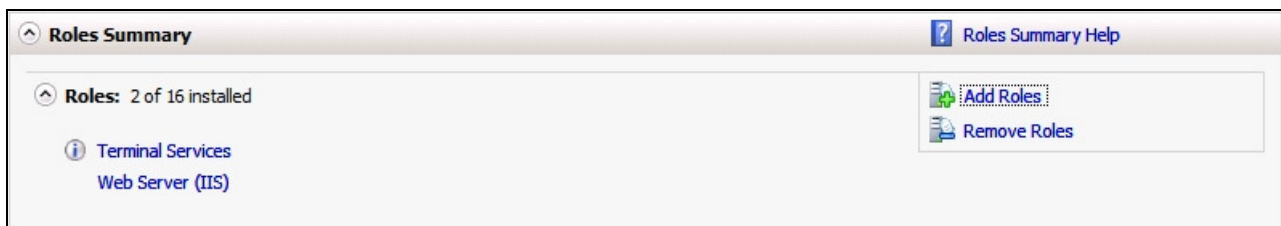


Figure 11 - Adding a role on Microsoft Windows 2008 Server

AppliDis requires the installation of a Microsoft Internet Information Services (IIS) Web server configured with:

- use of ASP pages.
- Windows authentication
- Microsoft Internet Information Services (IIS 6) management compatibility.

This configuration is carried out in the "**Server Manager**".

Access the menu **Server Manager - > Roles - > IIS Web server**.

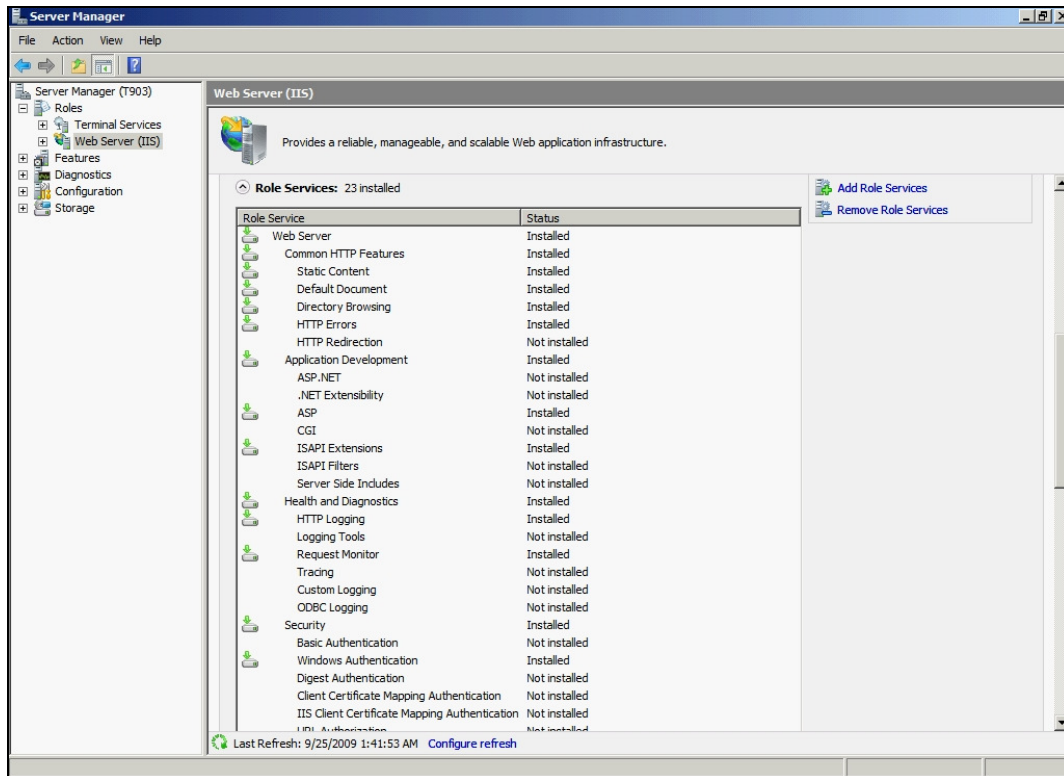


Figure 12 - Visibility of Internet Information Services (IIS) roles on Windows 2008 Server

Open the window to add role services (Link "**Addition of role services**" on the right-hand side of the window).

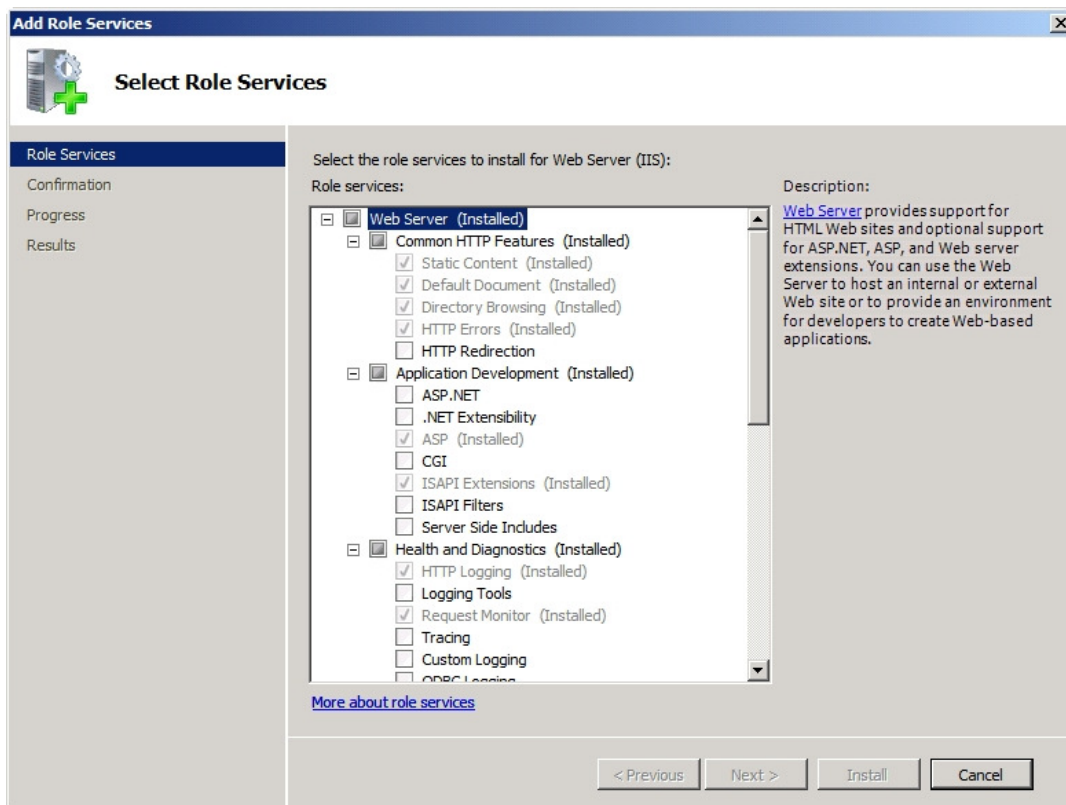


Figure 13 - Selection of IIS services to be installed on Windows 2008 server

Check that the following role services are installed and checked:

- **Web server - > Development of applications - > ASP**



- **Web server - > Security - > Windows Authentication**



- **Web server - > IIS6 Management Compatibility**



8.5 Configuration of Microsoft Terminal Services or Remote Desktop

This component provides a full desktop of the Windows 2000 Professional, Windows XP or Vista type for various kinds of connected terminals. This tool is available in the various versions of Windows 2000 Server, Windows 2003 Server and Windows 2008 Server. Its name changed with the Windows 2008 R2 Server version and has become Remote Desktop. However, it is covered by specific usage licenses; for more information on licenses or on Terminal Server (or Remote Desktop) services, please refer to the chapter on Terminal Server (or Remote Desktop) services, page: 245. You must therefore have an up-to-date client license when you deploy a Terminal Server (or Remote Desktop) server as an Application Server. If your environment only contains AppliDis Application Servers operating under a 2000 Server, a Terminal Services license manager under 2000 is sufficient. On the other hand, if you have at least one AppliDis Application Server under 2003, your management server managing the licenses for your domain must also be under 2003, since this can manage the licenses for any type of TSE client accessing an Application Server of the 2000 or 2003 Server type at the same time. The same applies to the 2008 server, which is able to manage 2000, 2003 and 2008 CALs.

There are two licensing modes for TSE CALs:

- by User (one CAL per user regardless of the client workstation)
- by peripheral (one CAL per client workstation regardless of the user)

Installing the Terminal Server services on Microsoft Windows 2000 Server

1. In the Start menu, click on Settings, then on Control Panel.
2. Select Add/Remove Programs, then Add/Remove Windows Components.
3. Check the Terminal Server services (**Erreur ! Source du renvoi introuvable.** on Windows 2000 Server) box. In the Details section, the essential item is Activate Terminal Server services.
4. Click on Next.
5. In the 'Installation method' section, you must specify Application Server mode (**Erreur ! Source du renvoi introuvable.**)
6. On the default privileges window for application compatibility, select the Authorizations compatible with users of Windows 2000 mode.
7. Click on Next to finish installation.



Figure 14 - Installation of Microsoft Terminal Server services on Windows 2000 Server



Figure 15 - Configuration of the operating mode of Microsoft Terminal Server services

The difference between the two modes of use lies in the fact that the first mode, "Remote administration mode", is intended for administrators for the installation and configuration of Windows 2000 servers remotely, and limits the number of sessions opened per server to 2, while the second mode, "Application Server mode", allows the deployment of applications on the servers and their use by users. AppliDis is based on the second mode.

Installing the Microsoft Terminal Server services on Microsoft Windows 2003 Server

1. In the Start menu, click on Control Panel
2. Select Add/Remove programs, then Add or Remove Windows Components.
3. In the window which opens, called the Windows Components Assistant, select the Terminal Server line.
4. A window will open, explaining that the use of Internet Explorer will be subject to the restrictions activated on your server for this program (by default, reinforced security is activated for Internet Explorer). Click on Yes.
5. Click on Next.
6. Click on Next after reading the Microsoft warning which is displayed.
7. Select an average or total security level depending on the operating privileges required by the applications to be installed on the server (such as writing to the registry, etc.). You can install a high level and then return to normal level after installation.
8. Click on Next.
9. Restart when this option is offered at the end of the installation

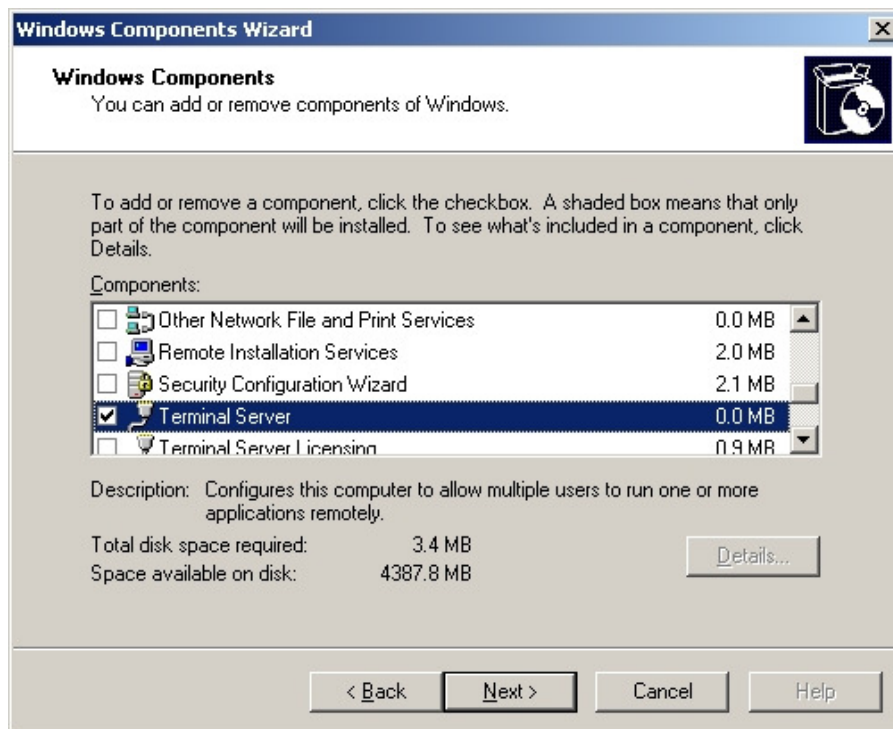


Figure 16 - Installation of Microsoft Terminal Server services on Windows 2003 Server

Installing the Microsoft Terminal Server services on Microsoft Windows 2008 Server

Check the **Server Manager** window to see if the **Terminal Server Services** role is installed.

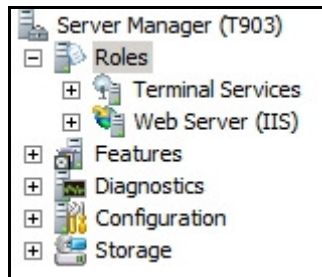


Figure 17 - List of roles in the Microsoft Windows 2008 server manager

This role can be installed from the "**Roles Summary**" sub-menu in the **Server Manager** screen.

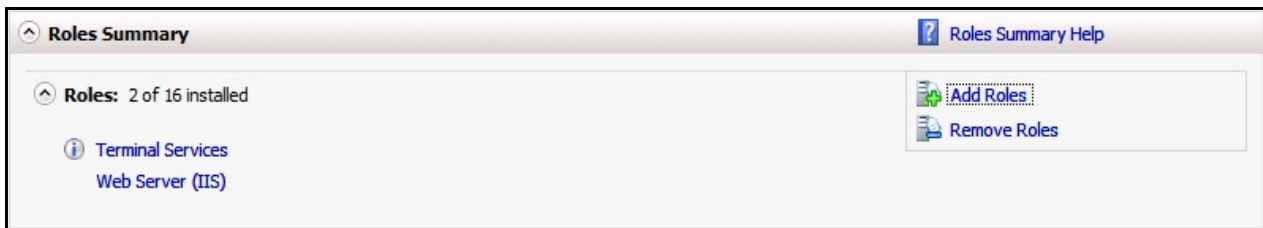


Figure 18 - Adding a role on Microsoft Windows 2008 Server

Configuration of the Microsoft Terminal Server service

Go to Start - > Administration tool - > Terminal Server Services -> Configuration of Terminal Server services.

Right-click on the line "**Restrict each user to a single session**", select "**Properties**" and check that the "**Restrict each user to a single session**" box is not checked.

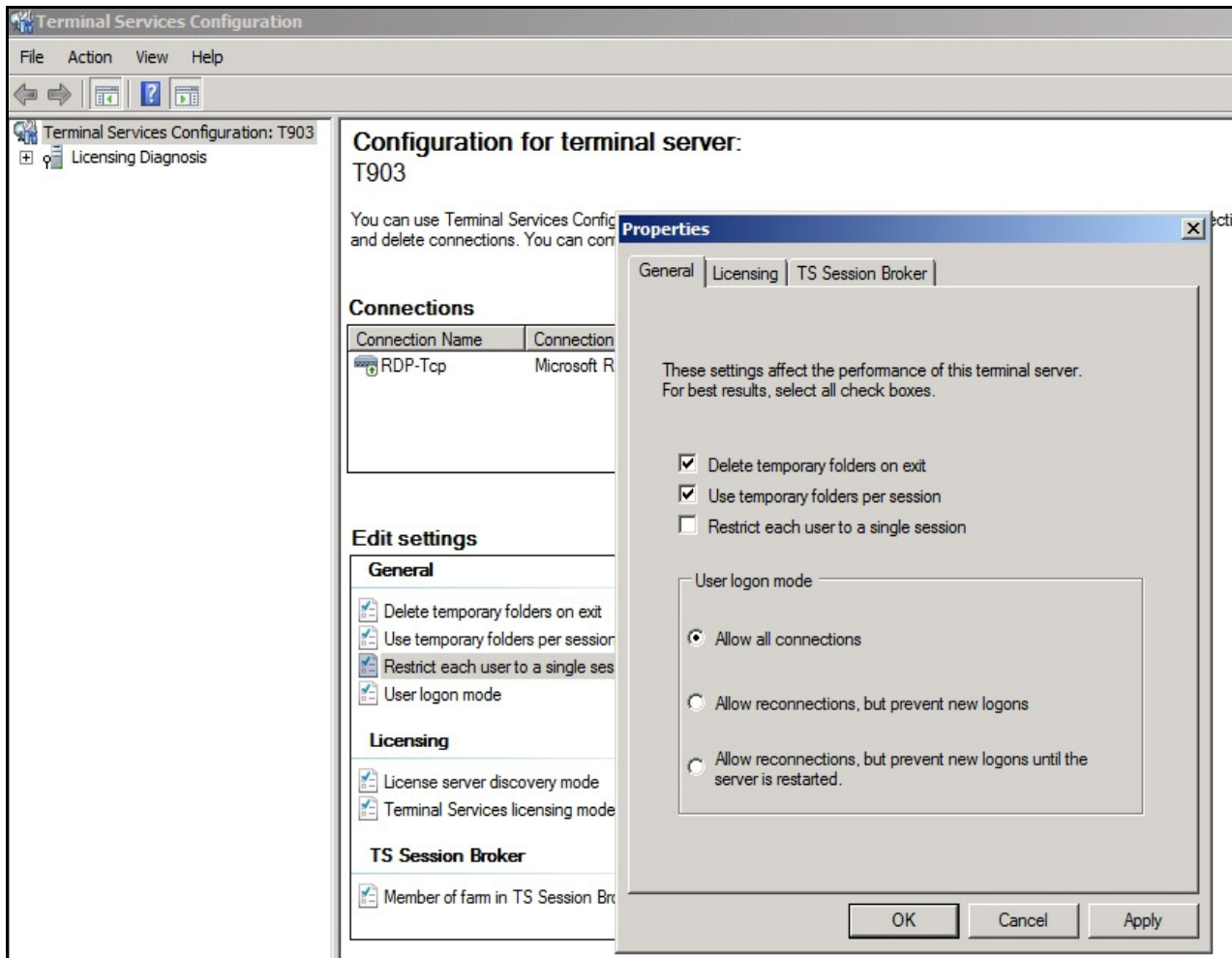


Figure 19 - Configuration of Terminal Server services on Microsoft Windows 2008 Server

Remote APP configuration for launching in application mode

Go to Start - > Administration tool - > Terminal Server Services - > Remote APP TS Manager.

On the line "**Terminal Server settings**" click on "**Edit**" and check that the "**Show a remote desktop connection to this terminal server in TS Web Access**" box is ticked.

Also ensure that the option "**Allow users to start both listed and unlisted programs on initial connexion**" is selected in "**Access to unlisted programs**".

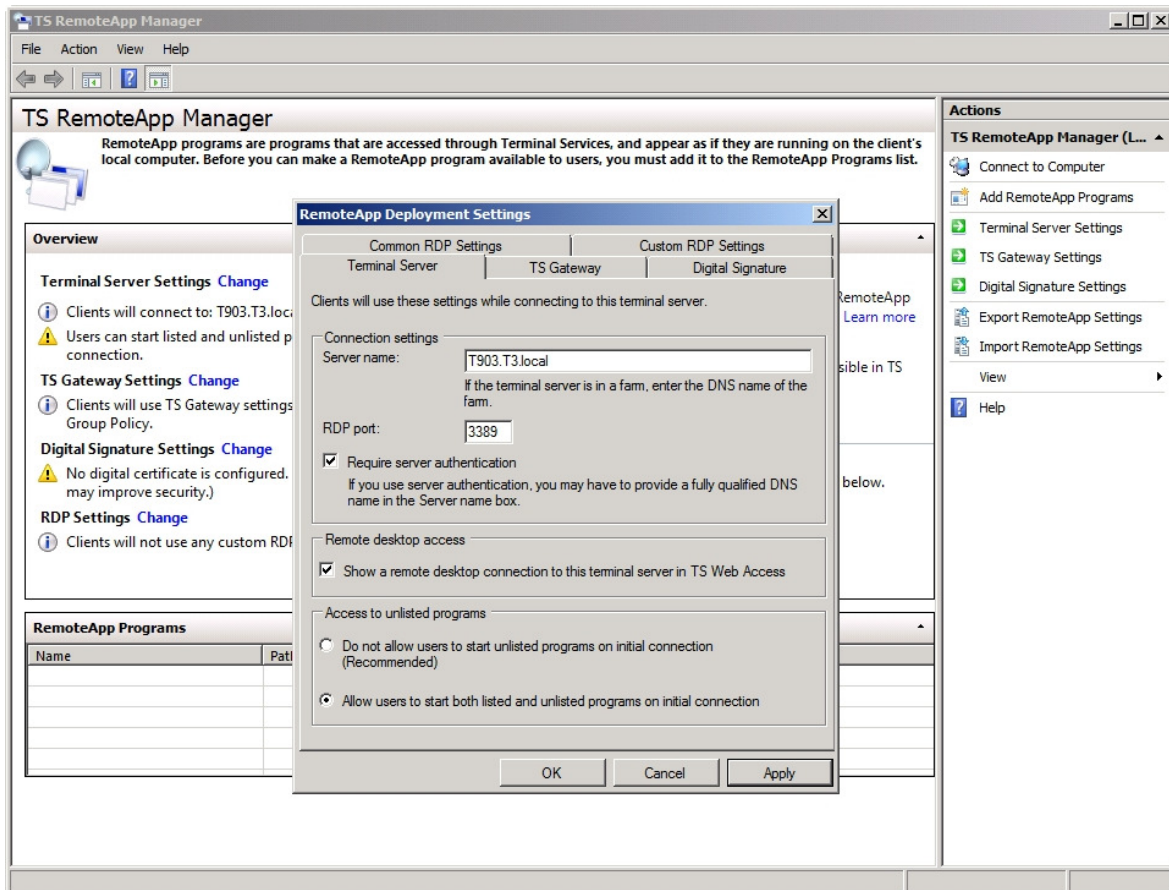


Figure 20 - Remote App settings on Microsoft Windows 2008 Server

Installing Remote Desktop services on Microsoft Windows 2008 Server R2

Check the **Server Manager** window to see if the **Remote Desktop Services** role is installed.

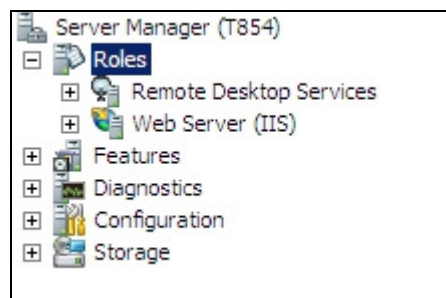


Figure 21 - List of roles in the Microsoft Windows 2008 R2 server manager

This role can be installed from the **"Roles Summary"** sub-menu in the **Server Manager** screen.

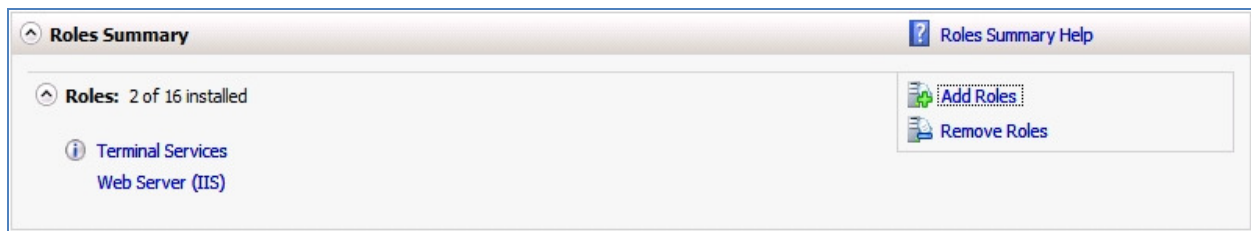


Figure 22 - Adding a role on Microsoft Windows 2008 R2 Server

Configuration of Microsoft Remote Desktop service

Go to Start - > Administration tool - > Remote Desktop Services -> Configuration of Remote Desktop session host.

Right-click on the line **"Restrict each user to a single session"**, select **"Properties"** and check that the **"Restrict each user to a single session"** box is not checked.

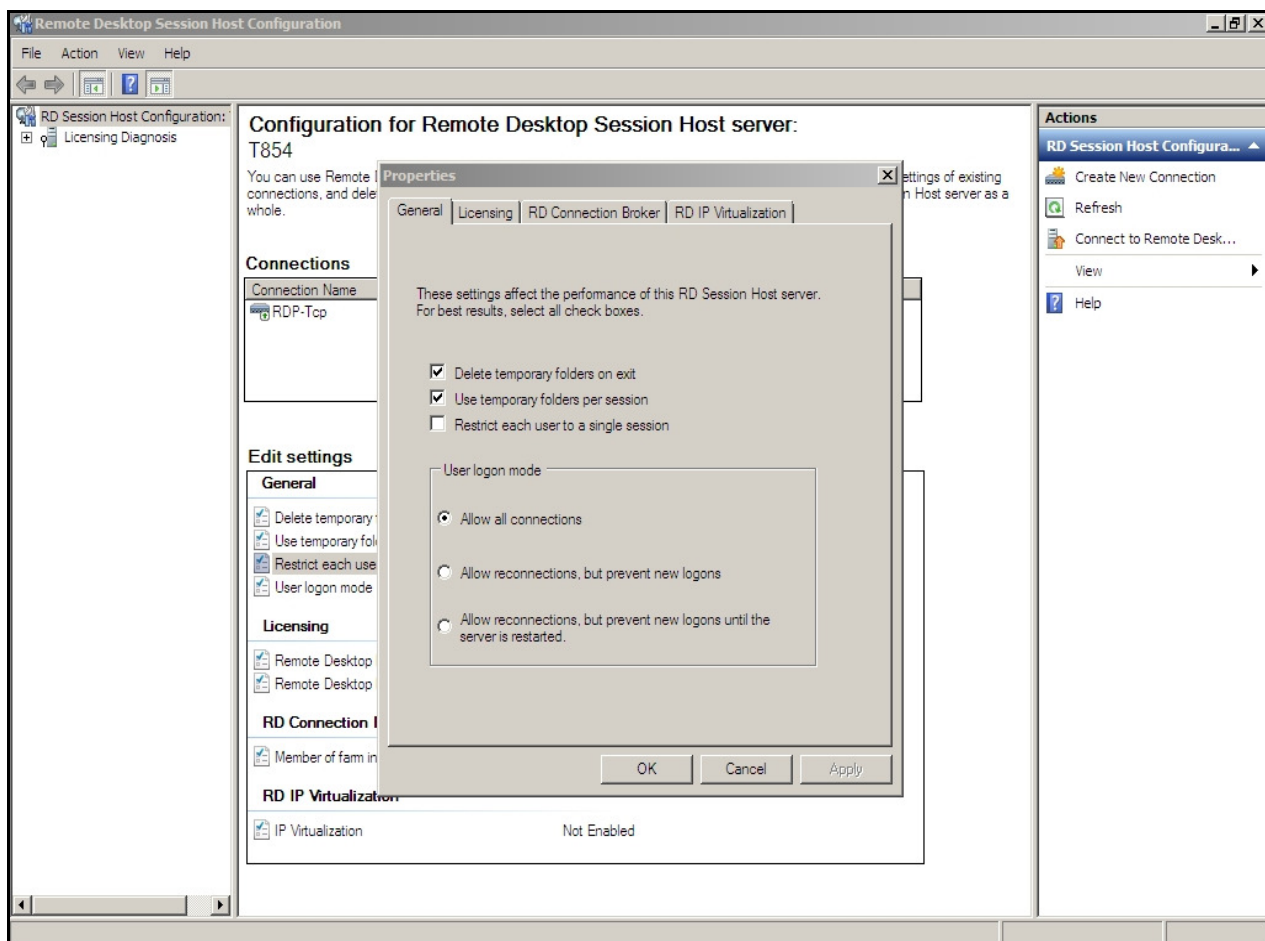


Figure 23 - Configuration of Remote Desktop services on Microsoft Windows 2008 R2 Server

RemoteApp configuration for launching in application mode

Go to Start - > Administration tool - > Remote Desktop Services - > Remote APP Manager.

On the line "**Remote Desktop session Host server settings**" click on "**Edit**" and check that the "**Show a remote desktop connection to this RD session Host server in RD Web Access**" box is checked.

Also ensure that the option "**Allow users to start both listed and unlisted programs on initial connection**" is selected in "**Access to unlisted programs**".

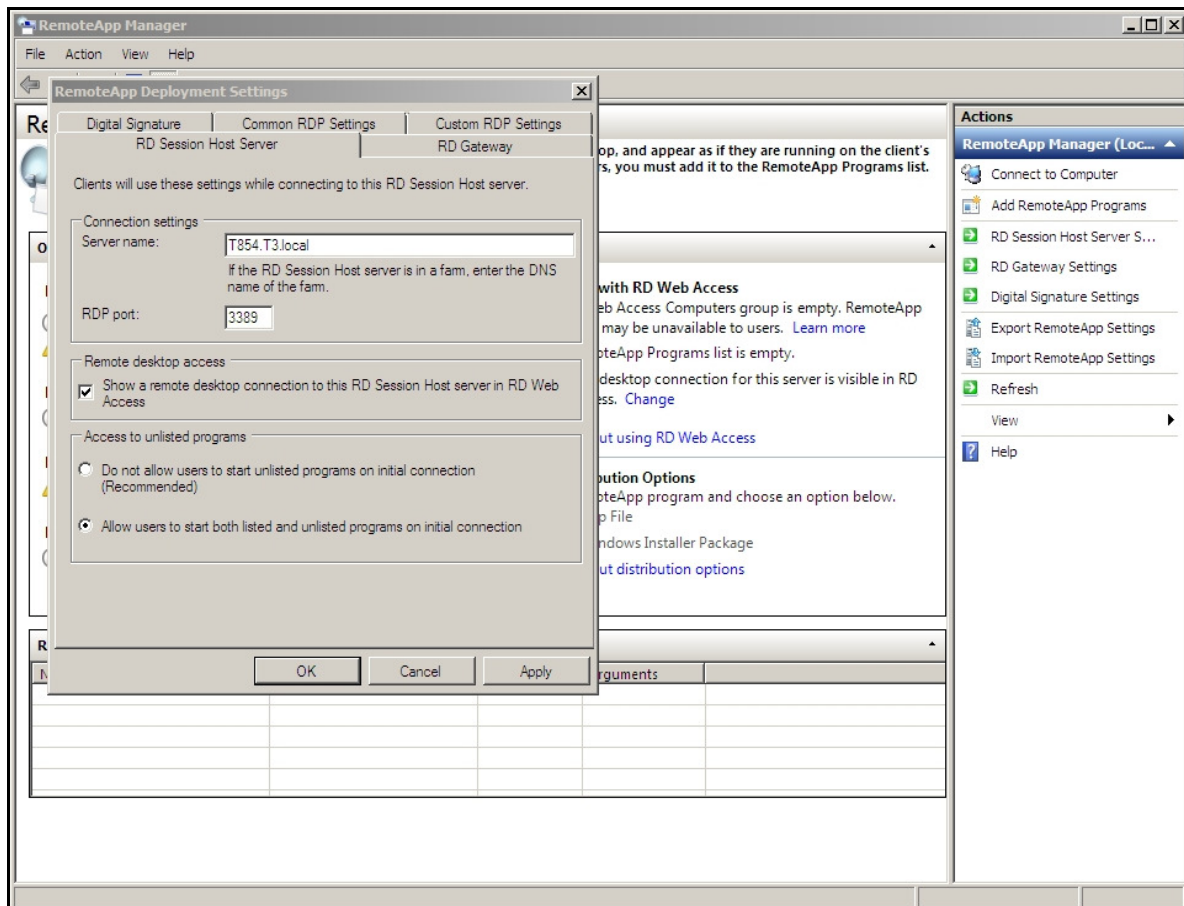


Figure 24 - Remote App settings on Microsoft Windows 2008 R2 Server

8.6 Fixed IP address

The AppliDis Administration Server and AppliDis Application Servers must have a fixed IP address.

Converting a dynamic IP address into a fixed IP address

These are the steps to follow to check that the IP addresses are fixed, including the procedure for switching to a fixed IP address if you are operating with a dynamic IP address (automatic IP address allocation). This check should be carried out on Windows 2000 Server and Windows 2003 Server operating systems.

1. In the Start menu, click on Settings (only under Windows 2000 Server; go directly to the Control Panel under Windows 2003 Server), then on Control Panel
2. Select Network Connections and remote access

3. Right-click on connection to your local area network. Select the Properties option in the pop-up menu.
4. Find the Internet Protocol (TCP/IP) in the properties for connection to your network. Select it then click on Properties.
5. In Internet Protocol (TCP/IP) properties (**Erreur ! Source du renvoi introuvable.**), make sure the Use the following IP address option is checked. If this option is already checked, it means you are already using a static IP address. Otherwise, enter a valid IP Address for your network, as well as a subnet mask and a default gateway.

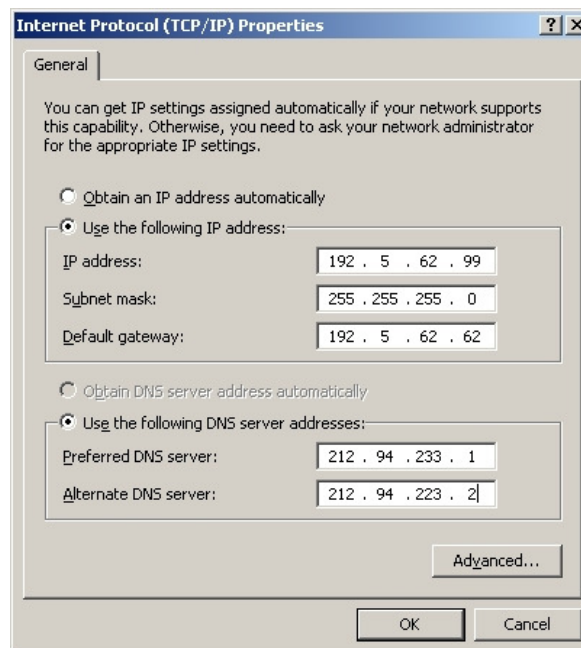


Figure 25 - Internet Protocol (TCP/IP) Properties

8.7 Installation of AppliDis on a domain controller

The installation of AppliDis on a domain controller requires a particular parameter setting and then needs to be restarted. The domain controller is configured to limit the access of users wanting to open a session. AppliDis users must be allowed to open a session on this device. It is therefore recommended that you create a user group in the Active Directory domain containing all the AppliDis users, if your users are managed by Active Directory. Moreover, AppliDis requires other privileges to be set to be able to function.

Configuring privileges for opening sessions on a domain controller

8.7.1 On 2000/2003 servers:

1. In the Start menu, click on Programs, then on Administration tools and finally on Domain Controller Security Strategy.
2. In the window which opens, click on Security Settings (left-hand list), Local Policies, User Rights Assignment, then in the right-hand list double-click on 'Allow log on locally' (Microsoft Windows 2003).
3. A window will be displayed with all the users that have this privilege. Click on Add to select the people or the group of people in your domain who will open remote sessions by using AppliDis.

4. In the window which opens, click on Security Settings (left-hand list), Local Policies, User Rights Assignment, then in the right-hand list double-click on '**Allow log on through Terminal Services**' (Microsoft Windows 2003).
5. A window will be displayed with all the users that have this privilege. Click on Add to select the people or the group of people in your domain who will open remote sessions by using AppliDis.
6. Click on OK to save your changes. Your Domain Controller must be restarted for the Settings to take effect.

8.7.2 On 2008/2008R2 servers

Installation of AppliDis on a domain controller 2008/2008R2 servers is not supported

9 Deployment scenarios

9.1 Simple configuration: one server and several clients

The minimal basic configuration to operate AppliDis consists of a Windows server on which one or more clients will be connected. The server will have the following roles:

- AppliDis Administration (installed from general AppliDis CD ROM)
- Application Server (installed from the administrative section of AppliDis)

This light configuration provides a simple way of implementing the AppliDis solution, although we recommend that the administrative section of AppliDis is located on another server, such as the company's Intranet server or the domain authentication server. This makes it possible to separate the execution of the applications (AppliDis Application Server) from their administration (AppliDis Administration Server).

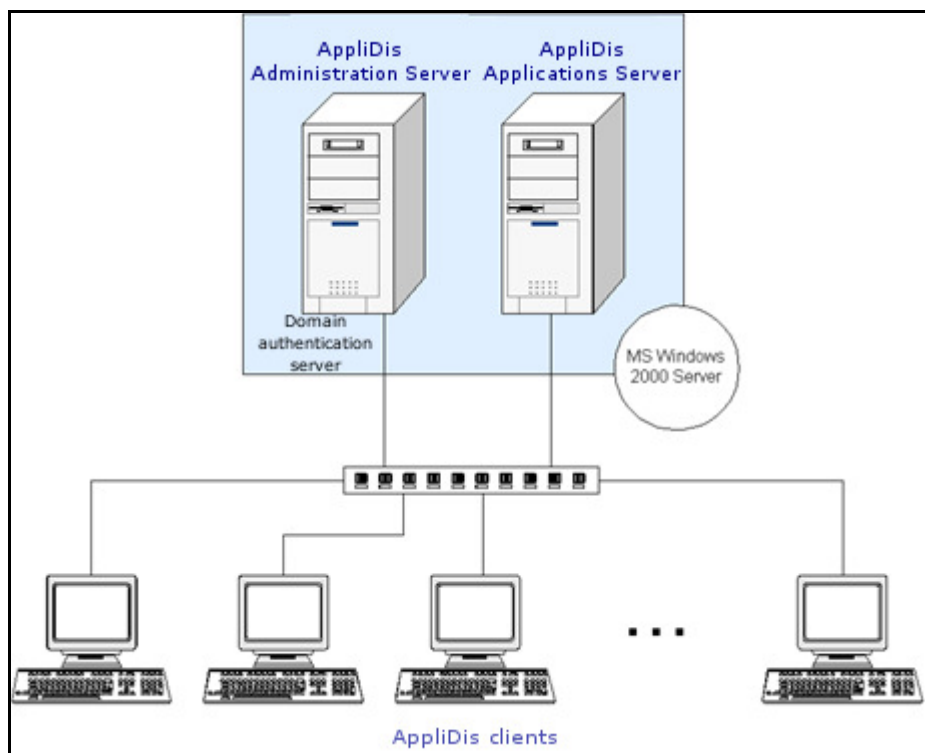


Figure 26 - Configuration with one Application Server and one Administration Server

9.2 Several servers with load balancing

A more secure configuration starts with the use of a second Application Server. This makes it possible to implement load balancing and provides redundancy, provided that the applications are installed on several servers. One of the Application Servers can also be the AppliDis administrator, although again, we recommend the use of a server other than an Application Server. The following diagram shows a configuration with several servers using load balancing.

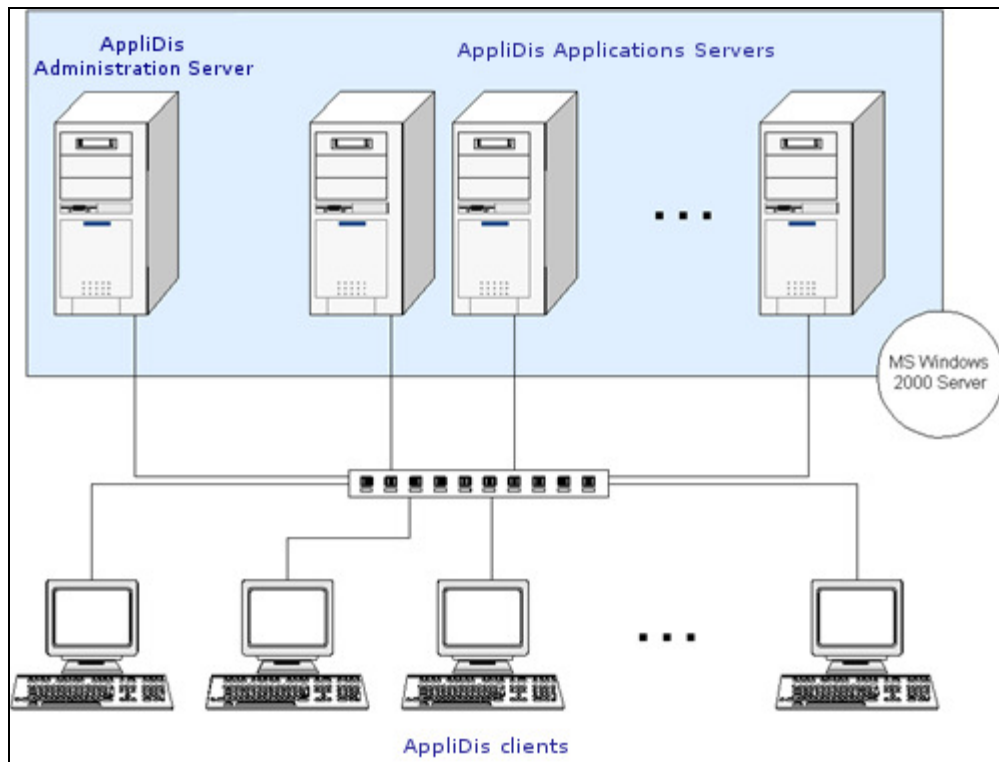


Figure 27 - Configuration with several application servers

Furthermore, please note that a system to protect against the "Black-Hole" effect is in place in the AppliDis load balancing engine. This makes it possible to artificially lower the grade of a server receiving a certain number of simultaneous connections. What may happen is that when the system is under load and a new unit is added, the new unit may be repeatedly selected by the load balancer, taking into account the imbalance of the calculated load. The server grade that is lowered in this way is valid until the server information is updated. Terminal Servers do not in fact readily support very fast session opening requests.

9.3 Redundancy of the Administration servers and application load balancing

Maximum continuity of service is ensured by the use of several AppliDis Administration servers. This redundancy is made possible by means of a virtual IP mechanism (IP Aliasing) managed by AppliDis.

This virtual IP address is carried by one of the Administration Servers. Should the server be unavailable, the virtual IP address will be carried by another AppliDis server which will take over automatically. The Administration Servers must be located in the same LAN. The virtual IP that you define must belong to the same IP network as your Administration Servers.

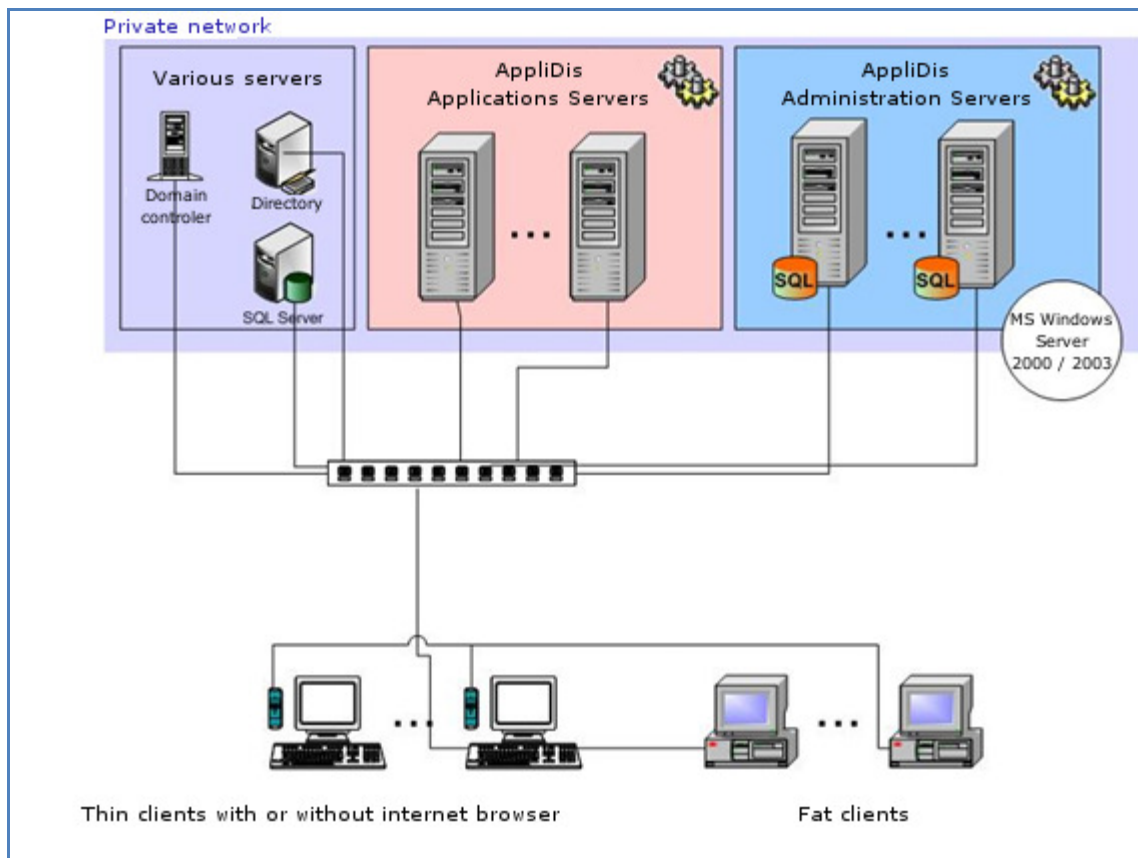


Figure 28 - Configuration with several administration servers

9.4 Configuration with a router for remote locations

AppliDis can also handle configuration with one or more remote locations. An example of remote configuration is shown in the diagram below. The AppliDis Servers (applications and administration) are located inside the Intranet network of the main site. Client workstations are located outside the network and are connected to AppliDis via a router. This configuration requires the opening of ports at the router level. To configure a solution of this type, please refer to page 87 ("Setting the IP address for configuration with router").

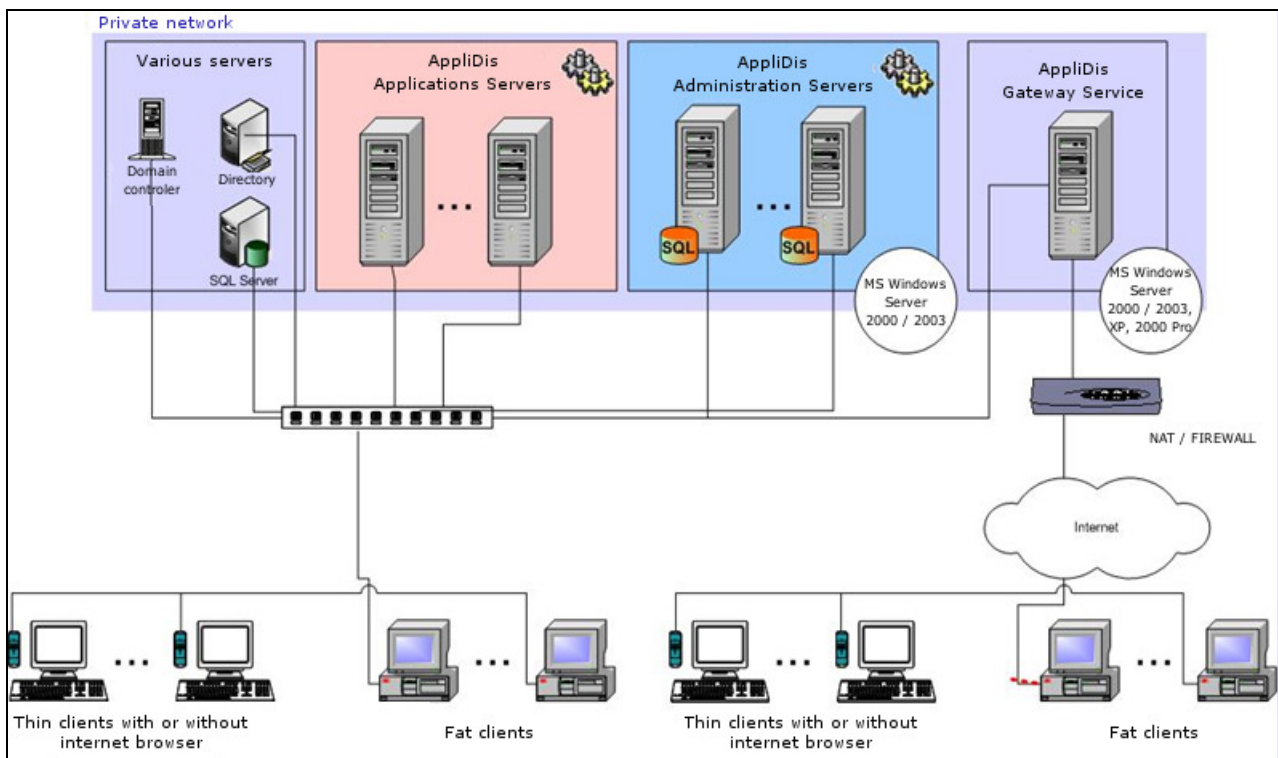


Figure 29 - Configuration with several administration servers, access by router and Gateway



Installing AppliDis

As soon as your servers are correctly prepared, the following step is to install AppliDis on one or more servers designated as AppliDis Administration Servers. For AppliDis in redundancy mode, it is recommended that you install your Administration Servers before deploying the other components.

10 Installation

10.1 Procedure

The procedures described below must be applied to **each redundant AppliDis administration server**. Open the AppliDis Administration console only when you are asked to do so. We will designate the first server on which we will install AppliDis as the Primary Administration server.

10.2 Installation of the AppliDis Administration Server

Starting the installation

Your target servers (Application, Administration or Gateway) must not have any AppliDis installations and must satisfy all the requirements described in this document.

It is necessary to be physically in front of the server or to be in TSE console mode.

Copy the AppliDis installation program into a folder on your hard drive, in a directory such as **C:\AppliDis-4** for example.

Switch your server to installation mode via "Add/Remove programs" or by running a command prompt (cmd.exe) and running the following command "change user /install". To return into the execute mode run the following command "change user /execute".

A screenshot of a Windows Command Prompt window titled 'Administrator: Command Prompt'. The window shows the following text: 'Microsoft Windows [Version 6.0.6001] Copyright (c) 2006 Microsoft Corporation. All rights reserved. C:\Windows\system32>change user /install User session is ready to install applications. C:\Windows\system32>change user /execute User session is ready to execute applications. C:\Windows\system32>_'. The prompt is at the end of the last line.

```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>change user /install
User session is ready to install applications.

C:\Windows\system32>change user /execute
User session is ready to execute applications.

C:\Windows\system32>_
```

Figure 30 - Command Prompt change user

Reminder: on a Microsoft Windows 2008 Server you must run cmd.exe as an administrator, by a right click "run as administrator".

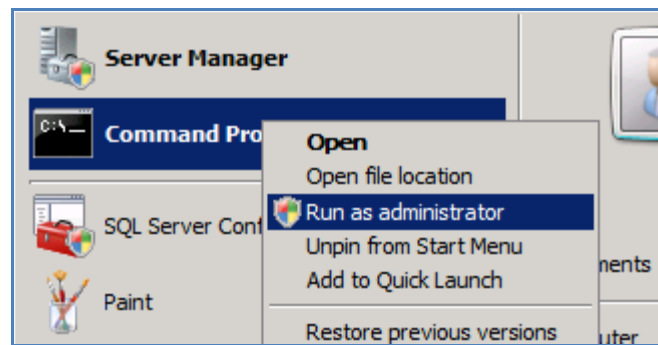


Figure 31 - Run as administrator

On a Microsoft Windows 2008, open the control panel (**Start -> Control Panel**), and launch **"Install Application on Terminal Server"**.

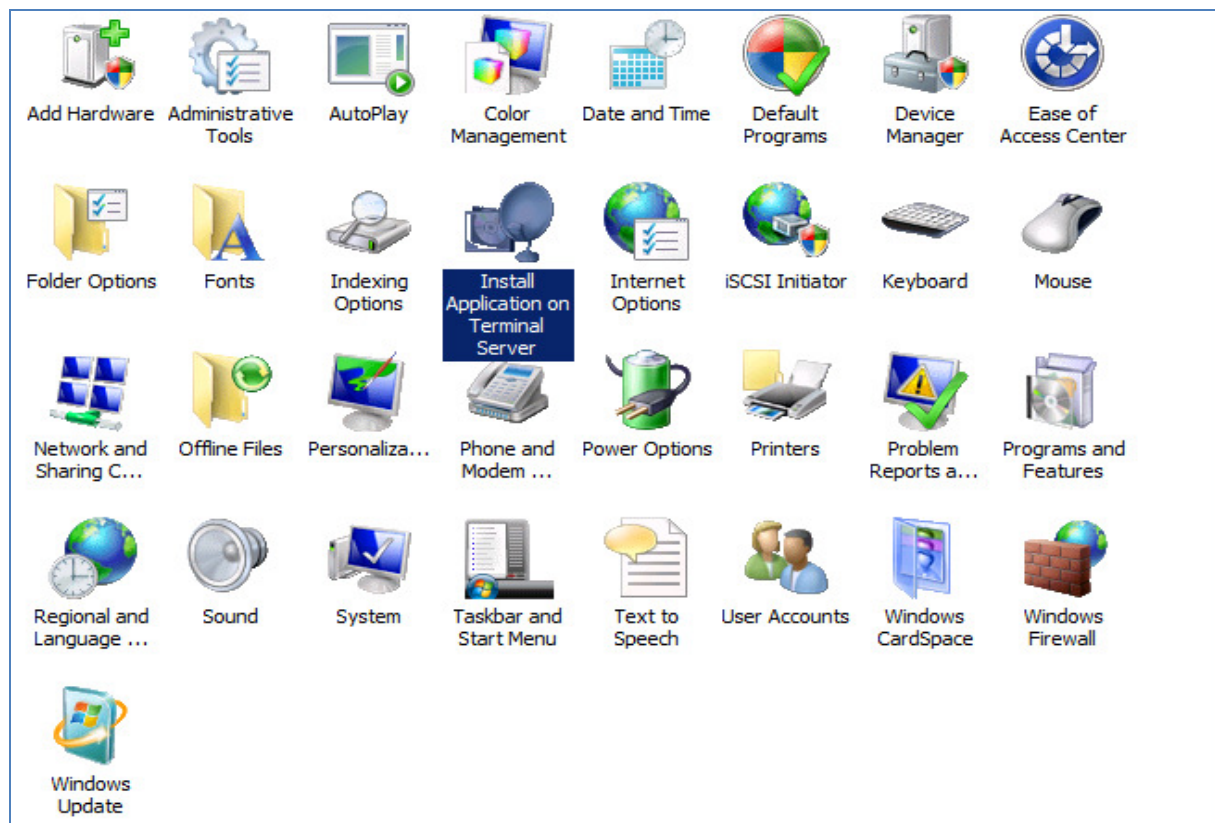


Figure 32 - Windows 2008 Install Application on Microsoft Terminal Server

Fill in the path to the **setup.exe** file from the AppliDis installation CD-ROM. Click on **next** and follow the AppliDis install shield.

Setting the installation directory

Set the AppliDis installation directory. This directory must be the same for each AppliDis administration server. When you deploy AppliDis components, they will be installed remotely using the same installation path as specified here.

Configuration of the main database type

Set the type of database which you will use for your local installation.

If you are installing your first AppliDis server, the "Creating a new AppliDis database instance" box must be checked. If not, uncheck this box so that the installation is linked to an existing database (when installing your second server, for example).

Note: The settings for redundancy of the AppliDis database (backup databases) are configured directly in the administration console. A backup database of a different type to the main database can also be defined.

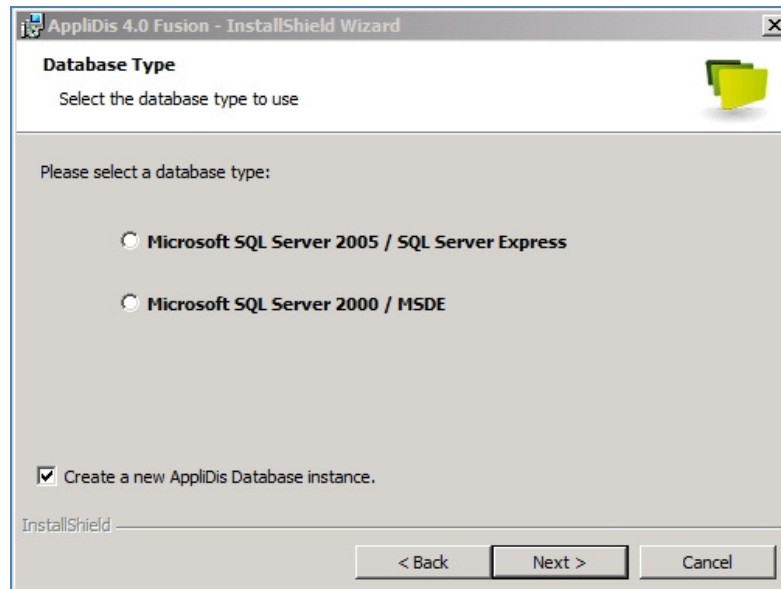


Figure 33 - Selection of database type

When this box is unchecked, the AppliDis installer assumes that the database already exists and will associate and register AppliDis with this database.

Configuration of a main Microsoft SQL Server database

Set the information for the main AppliDis database. This information must be defined in exactly the same way for each AppliDis administration server. Note these settings down or make a screen capture.

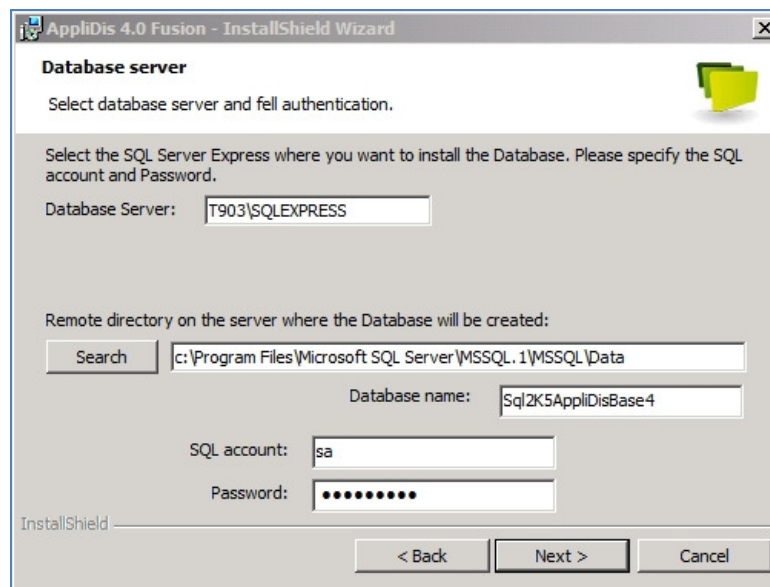


Figure 34 - Configuration of a Microsoft SQL database

Database Server

The Microsoft SQL Server on which you place the main SQL database. If your SQL server is installed in named instance mode, you must specify the instance in the name of the server, using standard notation, with the separator "\".

If, for example, your **SRVSQL1** server hosts an **INST2000** instance, specify the server name as: **SRVSQL1\INST2000**

Remote directory for database installation

Database path: Destination of Database files on the server.

Name of the Microsoft SQL database

Insert the name of the SQL database.

User information for SQL database access

- SQL user with System Administrator privileges on the SQL server.
- Password.

Configuration of a main Microsoft SQL 2005 or 2008 Express database

The settings for 2005 or 2008 Express databases are similar to the settings for SQL 2000 mentioned above; note, however, the configuration setting of the instance name **SQLEXPRESS**:

Microsoft SQL 2005 or 2008 Express instance name

When you install the SQL Server 2005 or 2008 Express, the instance is named **SQLEXPRESS** by default. Thus, the name of the server must be followed by the suffix **\SQLEXPRESS**.

For example, if your SQL server 2005 Express is called **SRVSQL2**, the name of the database server must be specified:

SRVSQL2\SQLEXPRESS

Configuration of a main Oracle 10g database

It is now possible to install AppliDis on an Oracle 10g database server to manage AppliDis data.

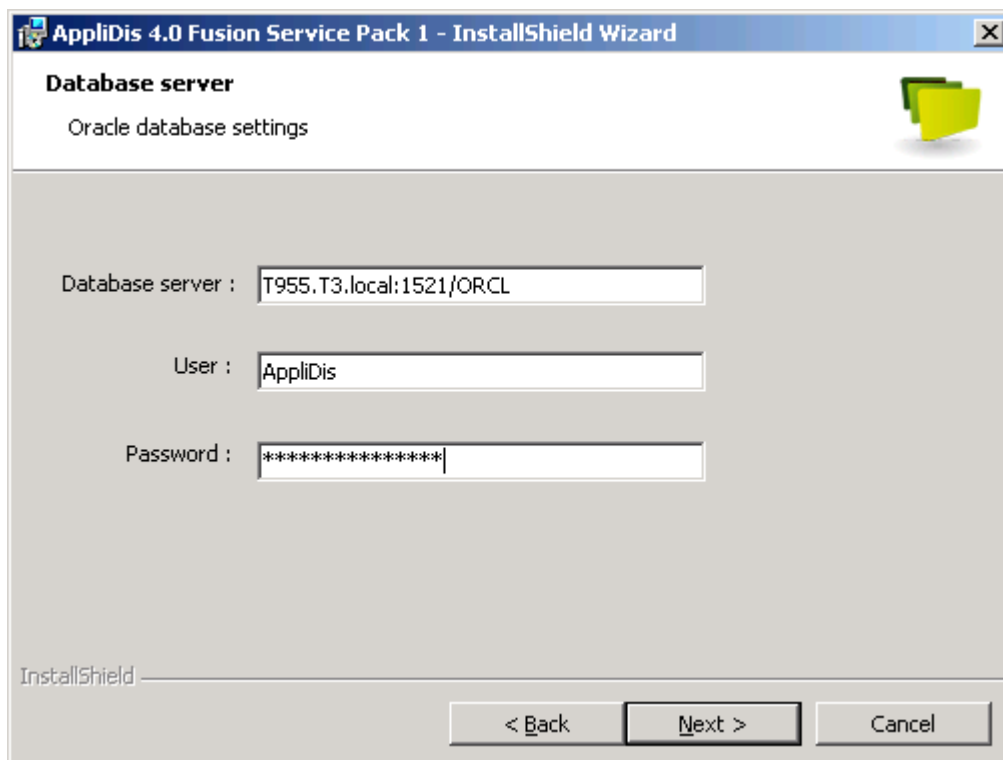


Figure 35 - Configuration of an Oracle 10g database

In the field "Database server", type the server name whilst respecting the following format: FQDN_ServerBDD:Port/Instance

Enter the administrator user name and the associated password, then click on "Next" to carry on with the installation.

End of the InstallShield wizard

Click on Next to continue file installation.

End of the Administration server installation

Your Administration server is now installed. If you wish to install an additional Administration server, you must install it immediately by repeating the steps above, otherwise skip it.

11 After installation

11.1 Start menu

The AppliDis installation program creates a **Systancia AppliDis** group in the programs group in the Start menu. Once this group has been created, you will have access to the following:

- Shortcut to the AppliDis administration console.
- Shortcut to the AppliDis applications portal

11.2 Post-installation configuration settings

AppliDis License

Enter the AppliDis license.

Directory

Configure the directory type in the Configuration/Directory menu if your user database is not of the NT4, Active Directory type.

Option

Uncheck Automatic registration of applications.

Load balancing

Check the box "**Priority to already open user sessions**" in the Configuration/Load balancing menu.

Virtual IP

Set the Virtual IP and check its operation.

To activate the monitoring module

Configure the settings for the AppliDis monitoring module from the AppliDis Administration console.

Backup databases

Set the AppliDis backup databases from the AppliDis Administration console (not available in demonstration mode).

11.3 Location of directories and files

When AppliDis is installed, several directories are created by default in the folder **C:\Program Files\Systancia**; the following is a detailed list of these directories:

Directory	Description
\AppliDis\AppliDis InstW2K8	Contains service for Windows 2008 servers.
\AppliDis\AppliDis Monitor	Contains the server monitoring agent (AppliDis Monitor service)
\AppliDis\AppliDis Redundancy	Contains the redundancy agent which manages the virtual
\AppliDis\AppliDisVDI	Contains the tree structure for the necessary components relating to VDI desktop management (Service, VDI Observer, Configuration tools)
\AppliDis\Base	Database (Foxpro format)
\AppliDis\Bin	All AppliDis programs and components
\AppliDis\Certificats	Certificate storage area for publishing a single application (for publishers only)
\AppliDis\DisFiles	Automatically generated files for AppliDis Client Desktop mode (AppliDis Client in desktop mode)
\AppliDis\Install	Contains the installation files of client components
\AppliDis\Lang	Files required to display the interface in French
\AppliDis\LogFiles	Automatically generated files for the monitoring of AppliDis administration (log book)
\AppliDis\Server	New server installation files
\AppliDis\Tools	Contains the AppliDis Launcher client, the Novell configuration tool and a database update tool
\AppliDis\Web	AppliDis websites
\AppliDis\WebServices	Contains the Web services files

An installed AppliDis Application and Virtual Desktop Host server has the following directories:

Directory	Description
\AppliDis\AppliDis Server	Server programs and components files.
\AppliDisClient	For virtual desktop and application host servers. Component and program files for servers (e.g. for virtual desktop).
\AppliDis\Printer	Useful components for universal printers by session.

An installed Gateway Server has the following directories:

Directory	Description
\AppliDis\AppliDis HTTP Gateway	Server programs and components files.
\AppliDis\AppliDis Gateway server	Server programs and components files.

An installed Web Users Portal Server has the following directories:

Directory	Description
\AppliDis\AppliDis Portal	Server programs and components files.

11.4 Uninstalling AppliDis

Before uninstalling AppliDis, you must uninstall all Application, Windows Desktop, Gateway and Web User Portal Host servers installed from the AppliDis administration console. No uninstallation of a virtual machine host server is necessary, because no AppliDis components are installed on those servers. However, it may be a good idea to delete clones created by AppliDis as needed.

Uninstalling AppliDis

To uninstall AppliDis, it is advisable to refer to card IS00069.

Uninstalling deletes all AppliDis user files

1. In the Start menu, click on Settings, then on Control panel
2. Click on Add/Remove programs
3. In the list, click on the Delete button in the AppliDis line
4. Click on OK to confirm your choice to uninstall AppliDis. The uninstallation ends by returning to Add/Remove programs.

Getting started with AppliDis Fusion

This chapter provides an overview of all the functions of AppliDis administration. Then, in order to start using AppliDis properly, the procedure for getting started quickly and easily under the best conditions will be explained. To this end, we will describe the steps to be followed to allow execution of an application via AppliDis and from a virtual desktop.

12 Navigating in the administration console

The administration console functions entirely via a Web interface.

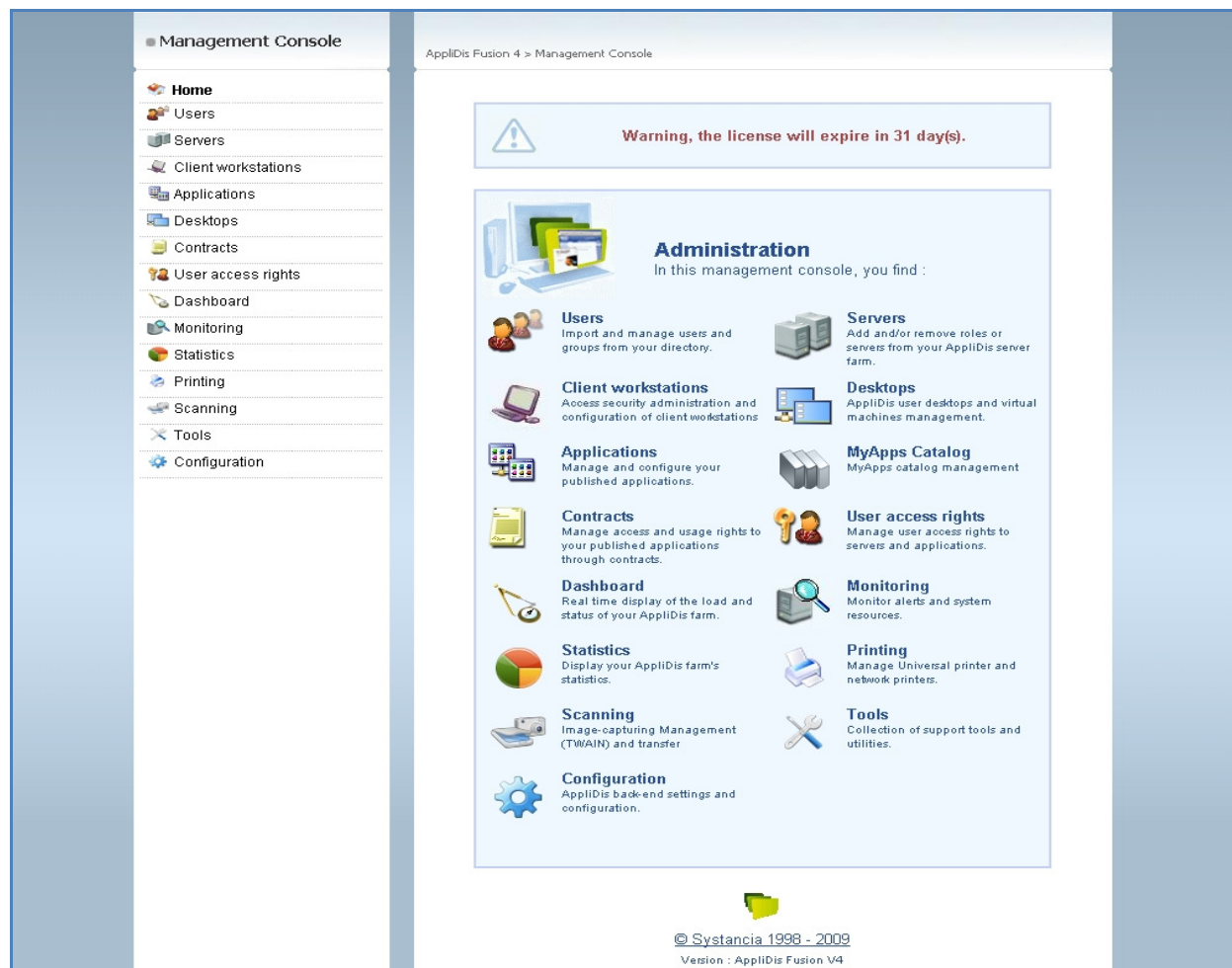


Figure 36 - Homepage of the AppliDis administration site

Users	User management: setting of groups and OUs in AppliDis from Active Directory, Novell NDS or another LDAP directory
Servers	Management of servers and groups of servers; access to their features and to hosted applications; Management of virtual machines; configuration of virtual IP address mechanism for administration servers; configuration of HTTP Gateway.
Client workstations	Management of security settings on the AppliDis virtual desktop: prohibition of application launch, non-accessible file types; assignation of client workstations to associated groups of servers.
Applications	Addition and management of applications used by AppliDis, early publication
Desktops	Management of desktops; access to their features; management of clones.
MyApps Catalogue	Using the MyApps catalogue, the administrator can provide a list of applications for users to consult. For their part, users request access to applications from this list and the administrator either grants or denies access to the requested application. In addition, users can leave a comment and/or a rating for the application to inform other users about the usefulness of the application.
Contracts	Addition and management of contracts, the elements binding users to applications, application groups or desktops
User access rights	Management of access privileges for users
Dashboard	Real time monitoring of server use; ability to activate or deactivate a given server.
Monitoring	Feedback of information from the servers in the farm (event logs, server characteristics –RAM / CPU / Disks, TSE sessions); management of configuration alerts; module for sending information by email
Statistics	Statistics on the use of AppliDis by monitoring servers, users, applications and desktops.
Printing	Configuration of universal printer; of universal printer by session; configuration of network printers.
Scanning	Configuration of a digital input peripheral such as a scanner, webcam or other peripheral offering acquisition via the TWAIN protocol.
Tools	Set of AppliDis tools enabling administrators to manage their server infrastructure
Configuration	Management of general AppliDis settings (location, license, administrator privileges, directory, options, weighting of load balancing, backing up and restoring the database, session scripts, refreshing the web interface, TWAIN, interface languages)

13 Using AppliDis in a few steps

Are you trying to get your AppliDis solution up and running quickly? The basic key steps needed to make the AppliDis solution operational are set out in this chapter. We will go on to describe all the options offered in the configuration and use of AppliDis below.

To start AppliDis from the AppliDis Administration Server

1. In the Start menu, click on the Site Administration icon of the Systancia AppliDis program group.
2. Internet Explorer will open, and an authentication page will be displayed
3. Enter your user name in the User name field and your password in the Password field. Only domain administrators can log in at this stage.
4. Click on the OK button.

To add a set of users from the directory (in Dynamic Management mode)

1. Click on Users in the main menu then go to the User groups sub-menu.
2. Click on Add a group or Add an organizational unit (OU) and select the group or organizational unit of the domain to be added to AppliDis (add this group in the list on the right).
3. Click on the OK button.

To import a set of users from the directory (in Synchronized Management mode)

1. Click on Users in the main menu then go to the User groups sub-menu.
2. Click on Import (OU) and select the group or organizational unit of the domain to be imported to AppliDis (add this group in the list on the right).
3. Click on the OK button.

To add a Windows Desktop and Application Host Server

1. Click on the List of Servers in the main menu.
2. Click on Add Automatically.
3. Select the server to be installed from the list of available servers by checking the relevant Application Server box.
4. Click on the Install button.

To add an application effortlessly

1. Start your application (on the device with the AppliDis server) just as you would usually do under Windows.
2. Click on Applications in the main menu.
3. In the list of the applications, click on Referenced Today; your application will be displayed after just a few seconds. When the application appears, click on it, then on the Add Contracts button in the main menu (Let your application run until AppliDis detects it).

4. A window will be displayed where the contract can be entered. Select the user group that you have just imported in the Group list.
5. Select a start date, an end date and a maximum number of users that can use the application.
6. Click on OK.

To use the application via AppliDis

1. Click on Disconnect in the main menu in order to leave the administration site.
2. You will be redirected to the homepage of the administration site.
3. Click on the 'Applications Portal' client site icon (blue colour)
4. You will be redirected to the homepage of the applications portal. Enter a login and password of a person belonging to the group or to the OU for which you created a contract.
5. A page will open with the icon and the name of the application for which you issued a contract. Click on its icon or name. A window will open asking whether you want to download a component named "AppliDisClient.cab". Click on Yes.
6. After a few seconds, the application executed remotely via AppliDis will be displayed on your screen.

To add a virtual machine host server

1. Click on the List of Servers in the main menu.
2. Click on Add virtual machine host.
3. Fill in the server connection information along with its type.
4. Click on the Next button.
5. The installation starts.

To add a virtual desktop

1. Click on Desktops in the main menu.
2. Click on the "New Desktop" button
3. Enter a Name and a description, as well as the clone launch type.
4. Click on the "Next" button
5. The location screen appears.
6. Click on the "New location" button.
7. Select the host, then select the master machine.
8. Enter the number of clones required in the "Pool size" area.
9. Click on the "OK" button.
10. Click on the "Next" button
11. Enter the information about the domain (Domain, domain administrator account, domain administrator account password (twice) and local administrator account password (twice).
12. Then click the "Next" button
13. If the summary is correct, click the "OK" button
14. Pool creation starts. Wait until creation finishes.

Administering AppliDis Fusion

AppliDis enables you to manage your servers, applications, desktops and users, and to review the use which is made of the software, by means of detailed statistics.

14 Accessing the AppliDis administration

Initially, only the administrator of the Windows domain can connect to the AppliDis Administration. Later, you can specify which users will be able to carry out administration actions with AppliDis.

Opening the administration console from the AppliDis Administration server

1. In the Start menu, click on the Site Administration icon of the Systancia AppliDis program group.
2. Internet Explorer will open, and an authentication page will be displayed
3. Enter your user name in the User name field and your password in the Password field.
4. Click on OK.

Opening the administration console from another workstation

1. Open Internet Explorer on the workstation on which you are connected.
2. In the browser address section, enter the server name followed by /AppliDis/administration, for example: **server/AppliDis/administration** or **http://server/applidis/administration**
3. Enter your user name in the User name field and your password in the Password field.
4. Click on OK.

It should be noted that in general, the lists and groups of users, servers, applications and desktops can be managed and filtered by the first letter (or figure) of the ID of the person or object.

15 User management

15.1 Operating principle

Various types of directories (Active Directory, Domain NT, OpenLDAP/Samba, Novell, etc.) can be managed with AppliDis. The term Directory is also used to refer to the user management system on which AppliDis is based.

Two operating modes are available for access to your directory:

- Users are managed dynamically in AppliDis from the Active Directory domain, from the Windows NT domain, or from a Novell or OpenLDAP directory.
- Users are managed in a synchronized way in AppliDis; this requires the importation and synchronization of the users contained in the groups and the Organizational Units of your directory. This mode is only recommended when your user manager is not very powerful. Only synchronization operations can access the directory. If this option is activated, the directory can only be called up upon user authentication.

In any case, AppliDis is not intrusive to your Directory. No modification (such as schema extension) is necessary. AppliDis is based on objects that are already available. Moreover, AppliDis only has read-only access to your directory. If your network is managed by an NT4 domain controller, only the features related to the security groups are available, since it does not manage Organizational Units.

Note: For directories of the NT Domain or Active Directory type, only overall security groups are managed. Universal groups, for example, are not managed.

15.2 User management by Synchronization

15.3 The synchronized mode of user management is activated if the "Dynamic user management" option is unchecked (see page: 184, "Active Directory

By default, AppliDis Fusion 4.0 selects the domain in which the AppliDis Administration & connection broker servers are located. However, AppliDis manages as well connections from other domains or even from multi-domains.

The user groups can connect to an AppliDis Fusion 4.0 farm from a different domain even if they keep authenticating to the domain they belong to. The main interest is to offer a farm of shared AppliDis Fusion 4.0 virtualized applications for companies which have multiple independent geographical sites.

When a user launches his Microsoft Internet Explorer, the Fusion 4.0 AppliDis web portal displays a domain field. From the drop down list users can select the domain they wish to get connected to.

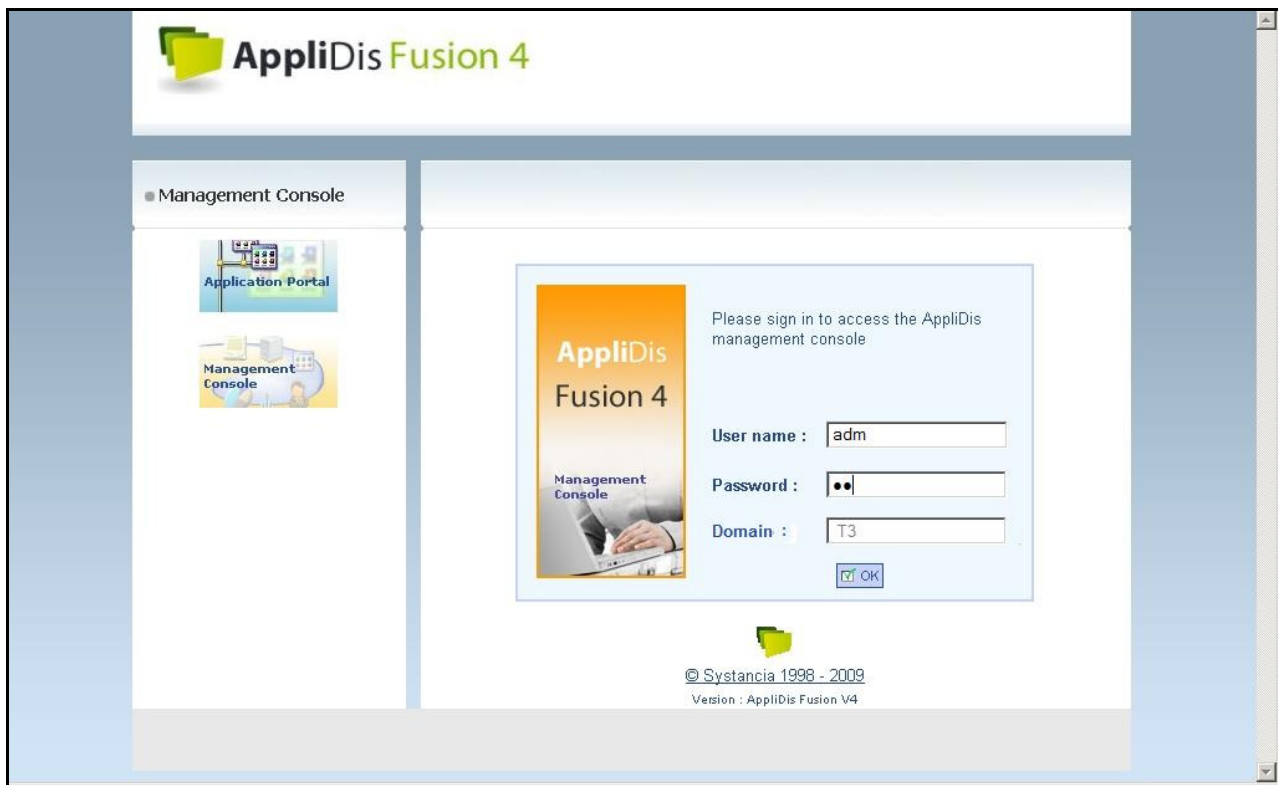


Figure 83 - Multi-domain authentication (AppliDis User Web portal)

All the requests to the Active Directory are established via the user account that connects to the AppliDis web client or to the Administration portal.

AppliDis Fusion 4.0 reads the active Directory information respecting rights of the user account that is part of the Active Directory.

For example, if a delegated administrator wishes to import Active Directory groups within AppliDis Fusion 4.0. If the user does not have access to those Active Directory groups, those groups in question will not be reachable & visible within the AppliDis Administration console.

Functionality Prerequisite

Users from approved domains must be added to the local Active Directory groups which are part of AppliDis Fusion 4.0.

Users must be authorized to get connected to Microsoft Terminal Server on the application hosts servers and Desktop windows.

Moreover, users must be part of the authorized user group which is entitled to get connected to Microsoft TSE.

Functionality Prerequisite

When installing AppliDis Fusion 4.0, the software is configured to import global groups & Organization Units (OUs). Furthermore, it is configured to read the Active Directory which is set with the ADSI mode. In this particular case, AppliDis Fusion 4.0 is linked to the Active Directory from which server AppliDis Fusion 4.0 is installed.

Activation of the multi-domain feature

Please navigate to configuration > Active Directory within the AppliDis Administration console, in order to check the type of available Active Directory. The two options are either ADSI or NetAPI.

Please tick the multi-domain management box in order to activate this feature.

As soon as the local groups are visible within AppliDis Fusion 4.0, they can be imported within AppliDis Fusion 4.0. Several algorithm solutions have been added in order to enhance the local groups search. It allows a greater flexibility & reliability when reading the Active Directory information.

The '**MemberSelection**' algorithm offers the possibility to grab local groups analyzing the **Member** properties of the user, thus discover all the user's local groups with his/her **domain\login** information.

The '**MemberOfSelection**' algorithm offers the possibility to grab local groups analyzing the **MemberOf** properties of the group, thus determine all the user's local groups.

The '**MemberSIDSelection**' algorithm offers the possibility to grab local groups analyzing the **Member** properties of the user depending on his/her unique SID.

The multi-domain management box is grayed out until you click on the top right corner arrow 'update directory connection'.

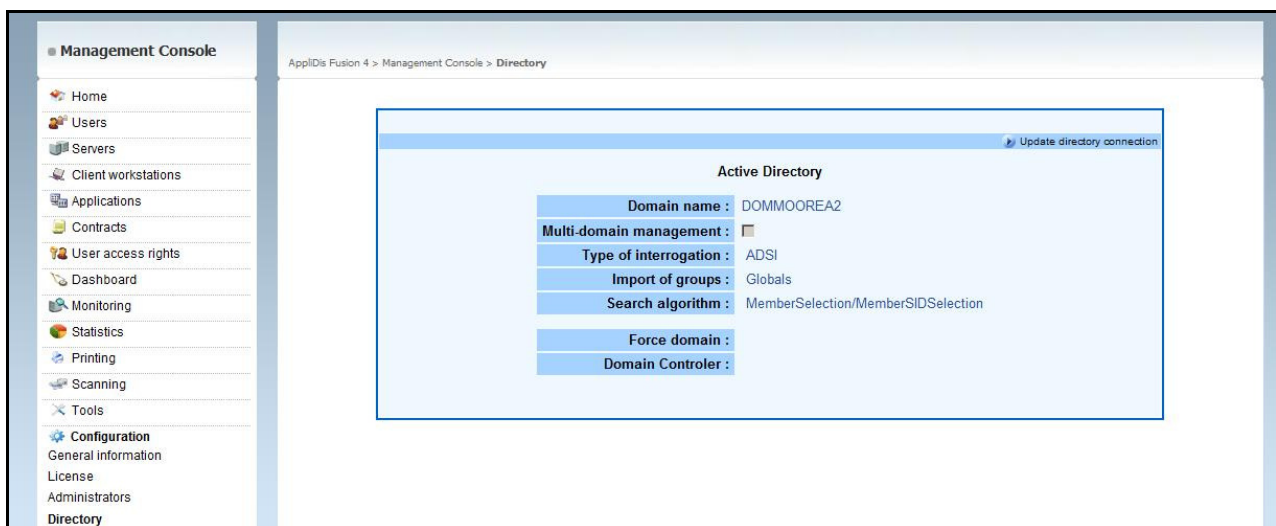


Figure 84 - Active Directory information

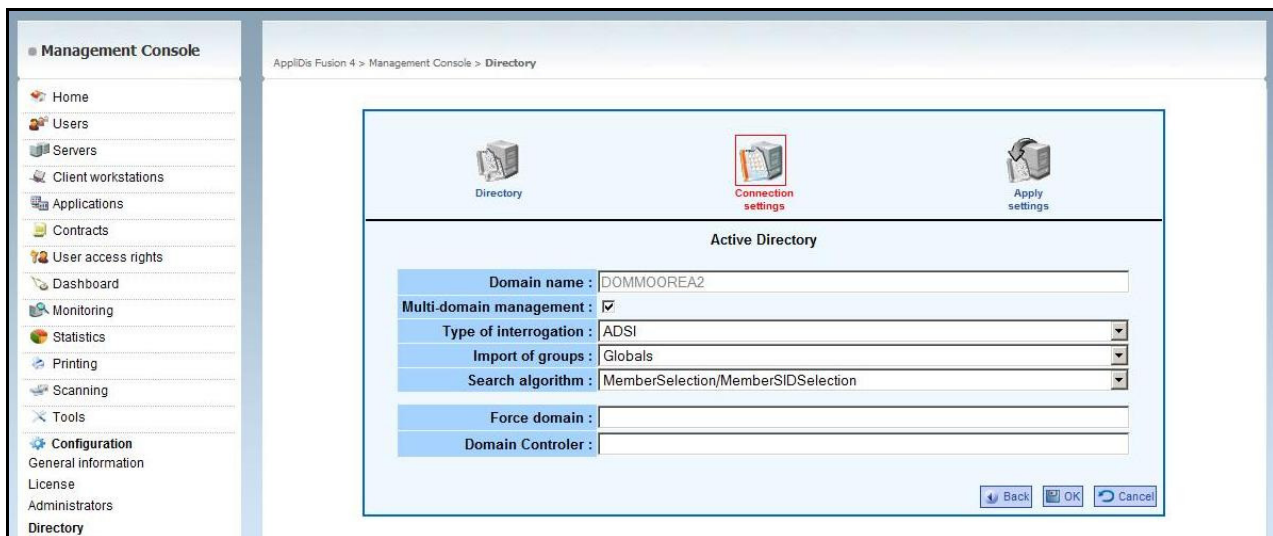


Figure 85 - Active Directory connection settings

1. AppliDis desktop & locked down clients are compatible with the two-way trust* mode.
2. The two-way trust options are available from the AppliDis Administration console (Menu > Configuration > Directory).
3. AppliDis Fusion 4.0 manages local groups which include intra-domain global groups running in NetAPI for the two-way trust mode.

* *One-way trust*: One domain allows access to users on another domain, but the other domain does not allow access to users on the first domain.
Two-way trust: Two domains allows access to users on both domains.

Configuration of the Active Directory options for a bi-directional access

From the AppliDis Administration console (Menu > Configuration > Directory), Administrators have the possibility to modify its configuration (see figure 77 above – Update directory connection). From within the connection settings menu (see figure 78 above), administrators can set & amend parameters.

The following table defines the various available parameters:

Multi-domain management	It activates the multi-domain management feature if the corresponding box is ticked.
Type of interrogation	(Active Directory Service Interface) ADSI or Microsoft Net API
Group imports	It defines the type of group within AppliDis for Microsoft NetAPI or ADSI

Algorithms (search function)	0 : Algo « MemberSelection » for both ADSI & NETAPI modes. 1 : Algo « MemberOfSelection » for both ADSI & NETAPI modes 2 : Algo « MemberSelection » for NETAPI & Algo « MemberOfSelection » for ADSI 3 : Algo « MemberOfSelection » for NETAPI & « Algo MemberSelection » for ADSI 4 : Algo « MemberSelection » for NETAPI & Algo « MemberSIDSelection » for ADSI 5 : Algo « MemberOfSelection » for NETAPI & Algo « MemberSIDSelection » for ADSI By default, the key is set to 4.
Domain Controller	Domain controller name (DC). It allows forcing the Domain controller. You must specify the domain controller with the IP address or the server name.
How to force the domain	It specifies the Netbios name. You must specify the domain name.

General options

AppliDis provides two options to create new groups in synchronized mode:

Importing a security group or an organizational unit in AppliDis

In synchronized mode, groups of users or the users of an OU in your directory must be imported into AppliDis. If modifications are made (addition or removal of users) the groups or the OUs must be synchronized again (this operation is described later on in this manual). The following steps are required in order to import a group or an organizational unit:

1. Click on Users in the main menu
2. Select User groups in the sub-menu.
3. Click on Import.
4. Select Security Group or Organizational Unit, according to the type of units you want to import.
5. In the list on the left, select the group or groups (or Organizational units) to be imported, then click on the right arrow to add the group in the list to be imported.
6. Confirm your selection by clicking on OK.

Note: When you import an organizational unit, you import all the users in the OU, including those located in sub-containers.

Creating an AppliDis group

In synchronized mode only, you can create an AppliDis user group, i.e., a group that is independent of your directory. You select the users that will be placed in the group yourself. This user group will not be reported in the directory and is not synchronized. Ensure, however, that you define a group name which is not used in your directory.

1. Click on Users in the main menu
2. Select User groups in the sub-menu.
3. Click on New group.
4. In the General Information page, put a name and description (optional), then click on Next.
5. In the list on the left, select the security group or Organizational Unit to list the users, then click on the arrow to add the selected users in the list on the right of users of the group.
6. Confirm your selection by clicking on OK.

Synchronizing groups and OUs

Once your various groups are in AppliDis, you can update them from the directory. This is necessary if users have been added to a group or organizational unit and if you wish AppliDis to be accessible to them. You can synchronize one particular group or all the groups present in AppliDis.

Synchronization consists of adding or removing the users of the group present in AppliDis in relation to the group or the organizational unit from which they came in the directory.

If a group has been removed from your directory after being inserted in AppliDis, it will not be removed during synchronization, but will then behave like a simple AppliDis group and will not be modified.

Synchronization of all groups

1. Click on Users in the main menu
2. Select User groups in the sub-menu.
3. Click on Synchronize.
4. You will be asked to confirm your request for synchronization: click on OK to accept.

Synchronization of a group

This option is only available on the groups from your directory, i.e. a group which you imported.

1. Click on Users in the main menu
2. Select User groups in the sub-menu.
3. Click on the group which you wish to synchronize (it will then be framed in red). Your Active Directory domain must comprise a group with the same name as this group to display the Synchronize group option.
4. Click on Synchronize group.
5. You will be asked to confirm your request for group synchronization: click on OK to accept.

Note: When you remove a user from your directory, a synchronization of the groups and OUs will eliminate this user from any groups to which it may have belonged. However, this user will not be removed from the list of users. This remains in the AppliDis users database, for statistical purposes, even if this user no longer has the means to connect to AppliDis.

15.4 Dynamic user management

Dynamic user management mode is activated if the "Dynamic user management" option is **checked** (see page 184, "Active Directory

By default, AppliDis Fusion 4.0 selects the domain in which the AppliDis Administration & connection broker servers are located. However, AppliDis manages as well connections from other domains or even from multi-domains.

The user groups can connect to an AppliDis Fusion 4.0 farm from a different domain even if they keep authenticating to the domain they belong to. The main interest is to offer a farm of shared AppliDis Fusion 4.0 virtualized applications for companies which have multiple independent geographical sites.

When a user launches his Microsoft Internet Explorer, the Fusion 4.0 AppliDis web portal displays a domain field. From the drop down list users can select the domain they wish to get connected to.

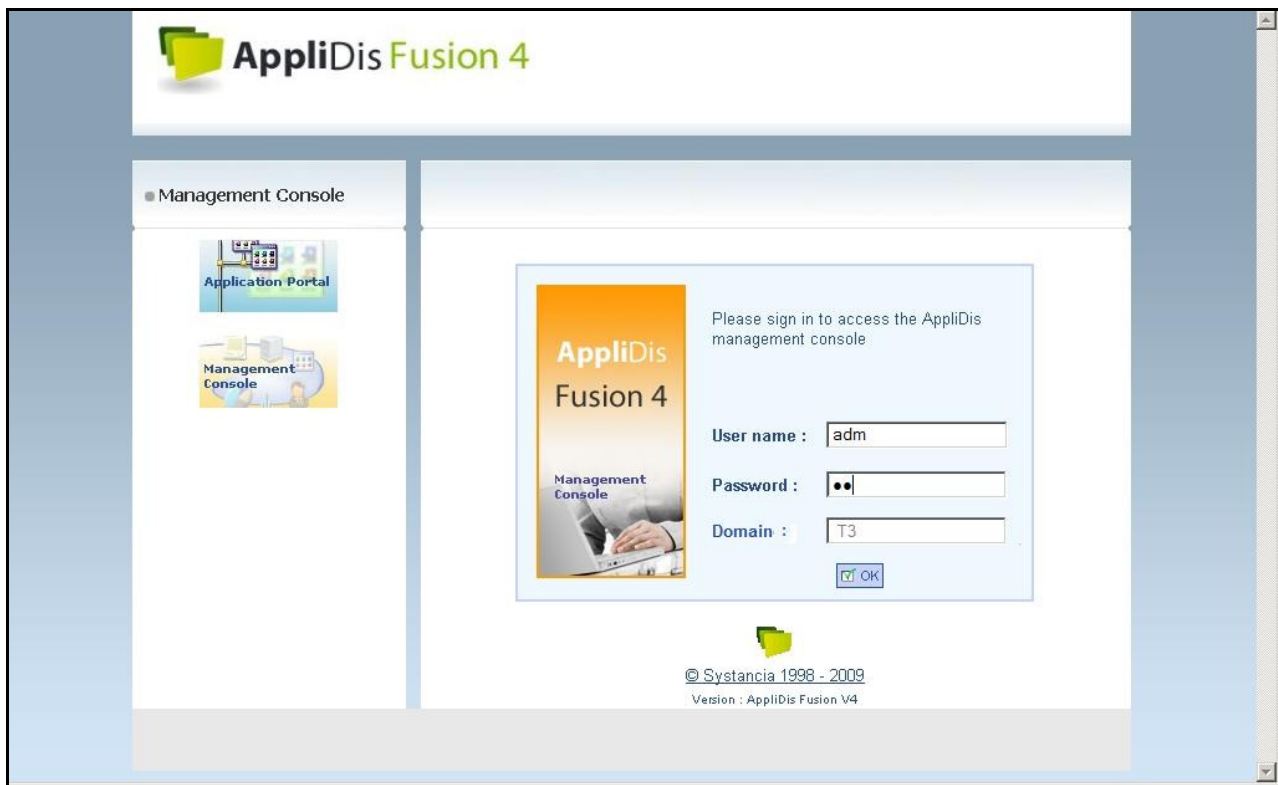


Figure 83 - Multi-domain authentication (AppliDis User Web portal)

All the requests to the Active Directory are established via the user account that connects to the AppliDis web client or to the Administration portal.

AppliDis Fusion 4.0 reads the active Directory information respecting rights of the user account that is part of the Active Directory.

For example, if a delegated administrator wishes to import Active Directory groups within AppliDis Fusion 4.0. If the user does not have access to those Active Directory groups, those groups in question will not be reachable & visible within the AppliDis Administration console.

Functionality Prerequisite

Users from approved domains must be added to the local Active Directory groups which are part of AppliDis Fusion 4.0.

Users must be authorized to get connected to Microsoft Terminal Server on the application hosts servers and Desktop windows.

Moreover, users must be part of the authorized user group which is entitled to get connected to Microsoft TSE.

Functionality Prerequisite

When installing AppliDis Fusion 4.0, the software is configured to import global groups & Organization Units (OUs). Furthermore, it is configured to read the Active Directory which is set with the ADSI mode. In this particular case, AppliDis Fusion 4.0 is linked to the Active Directory from which server AppliDis Fusion 4.0 is installed.

Activation of the multi-domain feature

Please navigate to configuration > Active Directory within the AppliDis Administration console, in order to check the type of available Active Directory. The two options are either ADSI or NetAPI.

Please tick the multi-domain management box in order to activate this feature.

As soon as the local groups are visible within AppliDis Fusion 4.0, they can be imported within AppliDis Fusion 4.0. Several algorithm solutions have been added in order to enhance the local groups search. It allows a greater flexibility & reliability when reading the Active Directory information.

The '**MemberSelection**' algorithm offers the possibility to grab local groups analyzing the **Member** properties of the user, thus discover all the user's local groups with his/her **domain\login** information.

The '**MemberOfSelection**' algorithm offers the possibility to grab local groups analyzing the **MemberOf** properties of the group, thus determine all the user's local groups.

The '**MemberSIDSelection**' algorithm offers the possibility to grab local groups analyzing the **Member** properties of the user depending on his/her unique SID.

The multi-domain management box is grayed out until you click on the top right corner arrow 'update directory connection'.

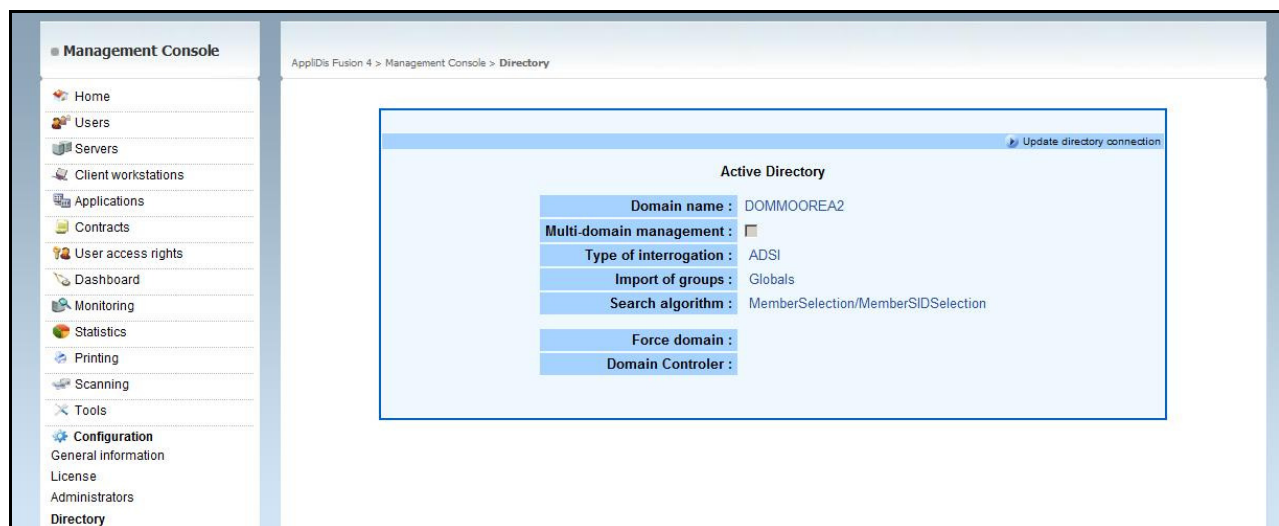


Figure 84 - Active Directory information

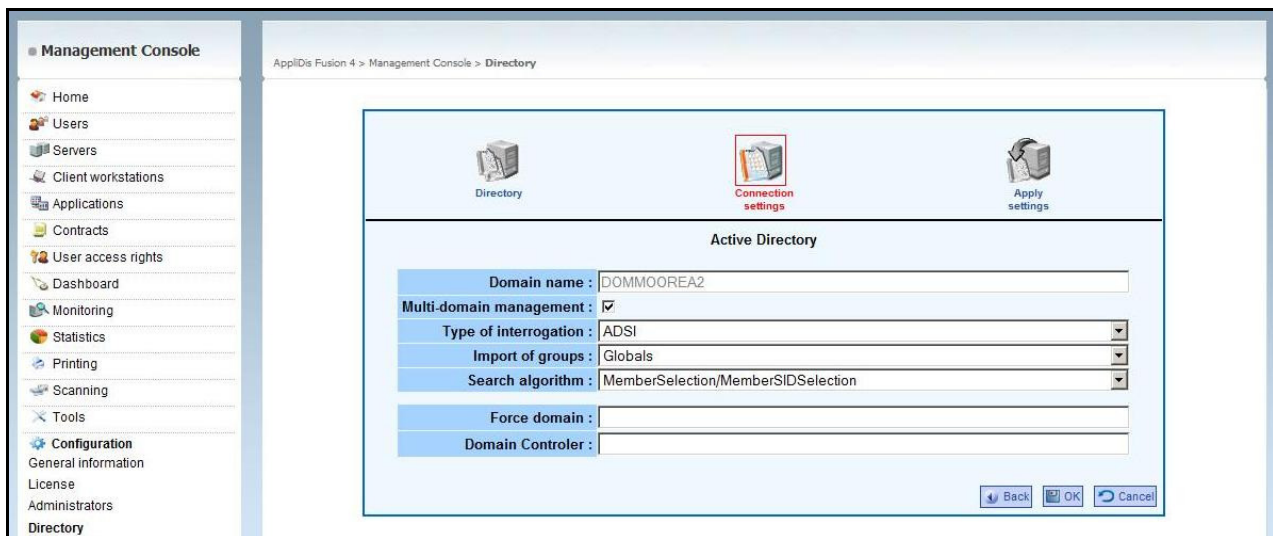


Figure 85 - Active Directory connection settings

4. AppliDis desktop & locked down clients are compatible with the two-way trust* mode.
5. The two-way trust options are available from the AppliDis Administration console (Menu > Configuration > Directory).
6. AppliDis Fusion 4.0 manages local groups which include intra-domain global groups running in NetAPI for the two-way trust mode.

* *One-way trust*: One domain allows access to users on another domain, but the other domain does not allow access to users on the first domain.
Two-way trust: Two domains allows access to users on both domains.

Configuration of the Active Directory options for a bi-directional access

From the AppliDis Administration console (Menu > Configuration > Directory), Administrators have the possibility to modify its configuration (see figure 77 above – Update directory connection). From within the connection settings menu (see figure 78 above), administrators can set & amend parameters.

The following table defines the various available parameters:

Multi-domain management	It activates the multi-domain management feature if the corresponding box is ticked.
Type of interrogation	(Active Directory Service Interface) ADSI or Microsoft Net API
Group imports	It defines the type of group within AppliDis for Microsoft NetAPI or ADSI

Algorithms (search function)	0 : Algo « MemberSelection » for both ADSI & NETAPI modes. 1 : Algo « MemberOfSelection » for both ADSI & NETAPI modes 2 : Algo « MemberSelection » for NETAPI & Algo « MemberOfSelection » for ADSI 3 : Algo « MemberOfSelection » for NETAPI & « Algo MemberSelection » for ADSI 4 : Algo « MemberSelection » for NETAPI & Algo « MemberSIDSelection » for ADSI 5 : Algo « MemberOfSelection » for NETAPI & Algo « MemberSIDSelection » for ADSI By default, the key is set to 4.
Domain Controller	Domain controller name (DC). It allows forcing the Domain controller. You must specify the domain controller with the IP address or the server name.
How to force the domain	It specifies the Netbios name. You must specify the domain name.

General options").

This operating mode is particularly recommended if the performance of your directory allows it.

In AppliDis in dynamic mode you can:

- **Add security groups.**
- **Add organizational units.**

Users are not imported. When a group or an organizational unit is added in AppliDis, the membership of the user to these entities is checked each time the user connects to an AppliDis server (from the portal, Desktop or any other AppliDis client).

Adding a user group

. The following steps are required in order to import a user group:

1. Click on Users in the main menu
2. Click on the Groups sub-menu.
3. Click on Add groups.
4. Under Novell, you must select the Organizational Unit containing the group.
5. From the list on the left, select the group or groups to be imported, then click on the right arrow to add the group to the list to be imported.
6. Confirm your selection by clicking on OK.

Note: In dynamic mode, any modifications carried out on a group in the directory will be reflected automatically in the AppliDis groups when connecting to the user's portal.

Adding an Organizational Unit

Organizational Units are the containers of your directory. When you choose to add an OU, all the users in this container and in the sub-containers are affected. Follow the steps below to add an OU:

1. Click on Users in the main menu
2. Go to the Groups sub-menu.
3. Click on Add Organizational Units.
4. Use Browse to select the OU you require. When the selection of the browser window is validated, the displayed list is positioned directly in the list on the left of the main window.
5. In the list on the left, select the Organizational unit(s) to be added, then click on the right arrow to add the OU group in the list to be added.
6. Confirm your selection by clicking on OK.

Note: One of the main advantages of dynamic directory management is that accesses to the applications can be managed directly in the accounts directory.

Example: The g_applidis_Word group provides access to the Word application via a contract in AppliDis. If I want to give access to this application to the user "user1", all I need to do is to add it in the g_applidis_word group in the directory.

Searching for a user

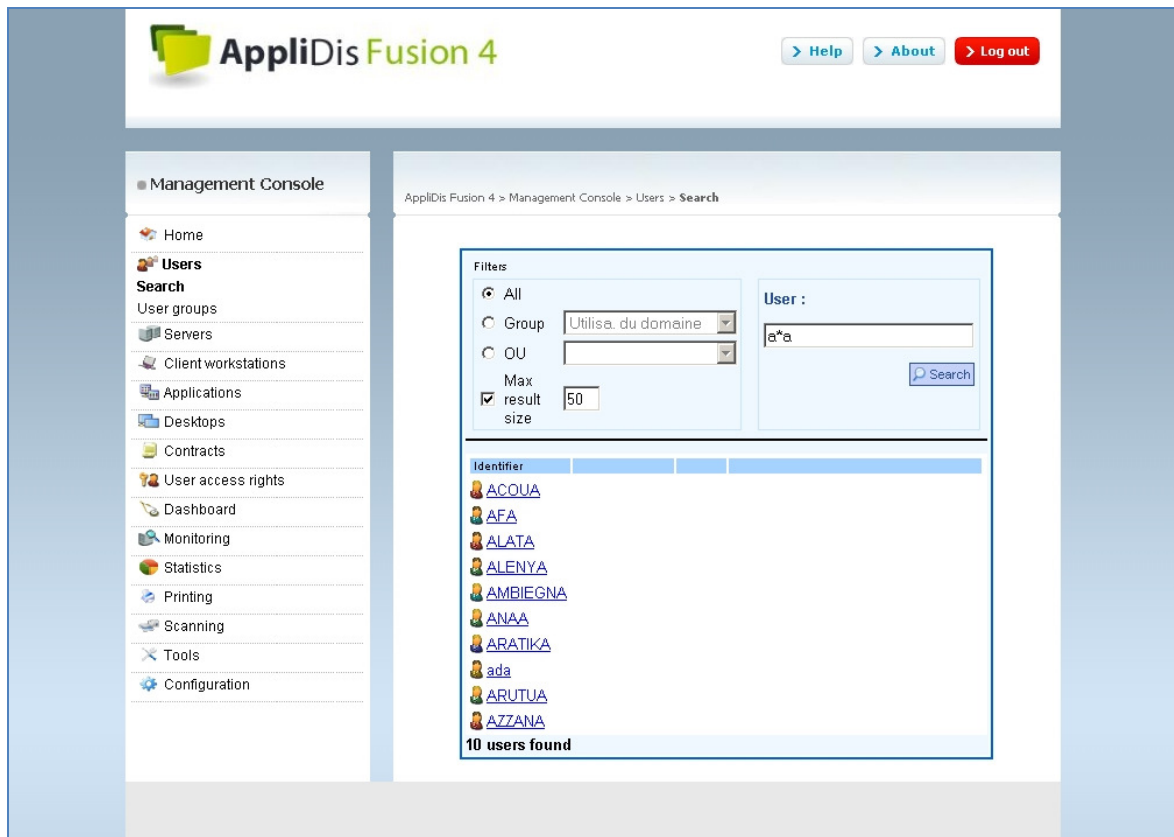


Figure 37 - AppliDis Administration Console (User search page)

You can search for a directory user to access and consult different options.

1. Click on Users in the main menu.
2. Click on Search
3. Enter a name in the User field. You can use the * character as a generic character.
4. You can set a filtering option, to search only in one group or one OU defined in AppliDis. You can also limit the size of the returned list.
5. The list of users corresponding to the request is displayed.
6. Select the desired user and click on Properties.
7. You can now review the characteristics, membership groups and options, the applications and the desktops.

15.5 Common user functions

The removal action enables you to make a user group disappear from the AppliDis administration. However, removing a group that was previously imported from a directory, **does not result in its removal** on your domain controller. Ensure that no contract is placed on the element before removing it. In the same way, ensure that the group or the OU that you are about to remove is not related to Delegated Administration.

Removal of an AppliDis group or organizational unit

You can carry out this action on both groups and Organizational Units imported from your directory.

1. Click on Users in the main menu.
2. Select User groups in the sub-menu.
3. Click on the group which you wish to remove (it will then be framed in red)
4. Click on Remove.

15.6 Redirection options for local disks, printers and permanent desktop option

Options for redirecting local disks, redirecting printers and accessing a permanent desktop can be configured at group and OU level, and also via the "User access rights" menu.

Options work according to an "add privileges" mode; that is, if an option is checked in one of the membership groups, the user will automatically be assigned the associated privileges.

You can use a user privileges report to check which options a given user is entitled to use. To do this, select your user by searching (see page 78 [Searching for a user](#)) and click on the "Properties" button. The properties for that user will appear. Click on the "Membership group and options" button, and you will be taken to a summary of the user's privileges.

Access to client workstation drives

By default, AppliDis users do not have access to their local disks (traditionally letter A: for the floppy disk, C: for the hard drive and D: for the CD-ROM). These disks can be redirected in order to make them available in the AppliDis client.

Once this redirection has been activated, a user of an application (e.g. Word) connecting from a client machine called "Sicily" performing the "Save As" action will be presented with a window showing disks A:,C:,D: of the server on which he/she is working in the form:

- A_\$ on ` Sicily', C\_\$ on ` Sicily' and D_\$ on `Sicily' classified in reverse-alphabetical order (thus A_\$ appears on a connected network disk called Z:, similarly, C_\$ appears on a network disk called Y, and so on) if the AppliDis Application server has a Windows 2000 Server operating system.
- A on SICILY, C on SICILY and D on SICILY classified in normal alphabetical order if the AppliDis Application server has a Windows 2003 Server operating system.

Note: When accessing an AppliDis Application server with a Windows 2000 Server operating system, access to client workstation drives is only available for Windows 95 and Windows 98 operating systems if Windows file-sharing is activated (refer to the AppliDis user's manual). On other client operating systems, users who use the access to their local workstations must be administrators of their client workstation. Furthermore, the client and the server must both be located in the same domain. However, when accessing an AppliDis Application server with a Microsoft Windows 2003 Server operating system, access to client workstation drives is always available for Microsoft Windows 95 and 98 operating systems even if Windows file-sharing is not activated. On other client operating systems, users do not have to be administrators of the device.

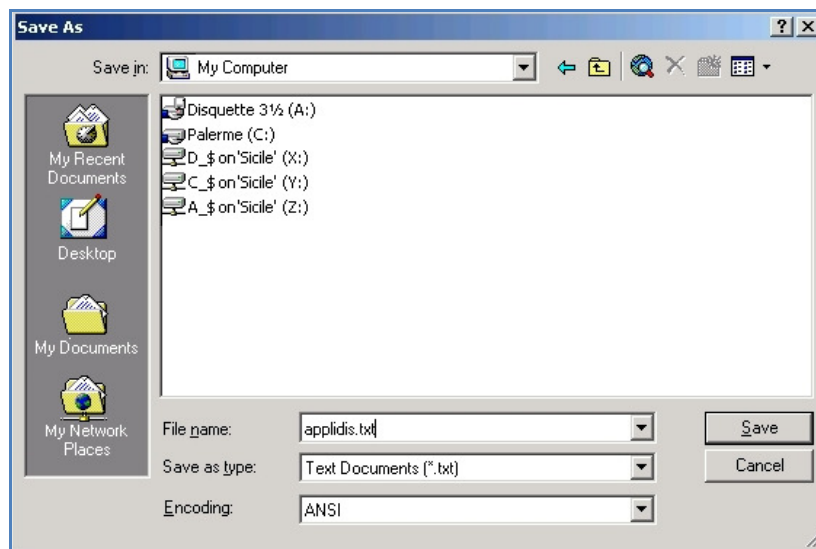


Figure 38 - "Save as" window showing access to local disks under Windows 2000

Access to local printers

In an application launched by AppliDis, your local printers are visible by default (cf. Printing with Terminal Server, page 247).

Permanent desktop option

When managing user groups, selecting a group (or OU) and then clicking on "Properties" will take you to information for the group. Clicking on the "Options" icon takes you to the available options for this group (or OU). You can check the "Permanent desktop" box then click the "OK" button to confirm your modifications.

When the "Permanent desktop" box is checked, users from this group will automatically have permanent desktops; that is, the desktops will not be reinitialised every time the user connects. The virtual desktop will then behave like an ordinary machine; users can make changes, alter settings and configurations, and even install applications. Each time the user reopens the desktop, it will appear just as the user left it at his last connection. Warning: although this mode is very intuitive and friendly for the user, it consumes large amounts of disk space.

If the "Permanent desktops" box is not checked, the virtual desktop is reinitialised every time the user connects. In this case, all modifications, customisations and installations are lost.

If the "Permanent desktops" privilege is not activated for a user who has already accessed a virtual desktop, and that user's privileges are then raised to "Permanent desktops", old desktops will be converted to permanent desktops.

Conversely, if the "Permanent desktops" setting privilege is activated, and that user has already accessed a virtual desktop and made modifications, and his privileges are lowered by the removal of access to his/her "Permanent desktops", the virtual desktop will then be converted to a non-permanent desktop after the last time the virtual desktop is switched off. If the administrator wishes to go back to an initial image, work is required to restore the snapshot on the hypervisor.

Configuring user group or OU options

1. Click on Users in the main menu.
2. Click on the User groups sub-menus
3. Select the user group for which you want to configure the options
4. Then select Properties
5. Click on the Options icon
6. You can then check the options that you want your user group to be able to access
7. Save your changes by clicking on OK

16 Server installation and management

16.1 Introduction

AppliDis server referencing principle

When you install an AppliDis server (an Application Host or Windows Desktop Server, a Virtual Machines Host Server, a Web Users Portal server or Gateway Server), it will be referenced in your list of AppliDis servers. You can then access the device's main information (RAM, hard drives, IP address and connection port for the Gateway- version, CPU, etc.). You can also create server groups to help configure access privileges for the groups or OUs.

Lastly, you will be able to access the applications available for a given application host and Windows desktop server and put contracts on these applications, thus providing your users with the option of executing the application remotely from this server.

In the same way, you can access available desktops for a given virtual machine host server and put contracts on these desktops, thus enabling your users to connect remotely to a virtual machine hosted on this server.

Summary of AppliDis Fusion 4 roles

As we saw in the previous chapter, there are a number of roles for AppliDis servers. Below is a summary of the various roles which exist for AppliDis Fusion 4

Role	Description
Administration and connection broker	The "administration and connection broker" role, as its name suggests, has two key functions: - First is the administration role, which is the heart of the AppliDis system and manages the whole of the AppliDis server farm. This role controls all of the other servers and also user access privileges. - Secondly, its connection broker role enables it to manage virtual machines and govern the creation of pools of desktops.
Web User Portal	The Web User Portal role simply enables the publication of the client portal site. Note: the administration server is also a Web User Portal server.
Gateway server	The Gateway server has two sub-roles: - an RDP gateway sub-role, enabling load balancing of virtual desktops for thin clients

Applications host and Windows desktops	Allows published applications to be run, but also makes it possible to access a full Windows desktop
Virtual machines host	Allows the various virtual machines available to users to be run in accordance with their privileges
	- an HTTP gateway sub-role, enabling the RDP protocol to be encapsulated within the HTTP protocol and thus provides AppliDis services through a firewall for Internet access for published applications

16.2 Administration and Connection Broker server

An Administration and Connection Broker server must be installed in accordance with the installation procedure: see the [Installing AppliDis](#) chapter.

16.3 Web User Portal server

A Web User Portal server is installed on a server which already has the IIS component installed. By default, an Administration and Connection Broker server is also a Web User Portal server.

16.4 AppliDis Gateway

Gateway and load balancing for thin clients

If the network comprises thin clients and several AppliDis Application servers are deployed, load balancing can be set up between these servers using the Gateway Server.

The connection mechanism is as follows: thin clients send requests for opening Terminal Server sessions to the Gateway device (which does not need to have the Terminal Server installed). The Gateway then polls the AppliDis administrator in order to find the best AppliDis Application server available for this thin client (load balancing) and then redirects the opening of the Terminal Server session to that best server.

If no AppliDis Application server is available, the request to open the session is stopped. A connection message to the server is then displayed on the thin client.

This solution is set up in the following way:

1. Install a Gateway Server (see Installing a server p.85)
2. You do not have to check the Gateway option in the configuration menu and option sub-menu (cf **Erreur ! Source du renvoi introuvable.** p.**Erreur ! Signet non défini.**) since in this case you will only force thin clients to connect to the Gateway without obliging other AppliDis clients (executed from the applications portal or Desktop mode) to use this mode
3. Then configure your thin client's Terminal Server client so that it connects to the Gateway device. To this end, launch the connection to the Gateway device (by using its name or its IP) on all the thin clients and enter the following start program: **BureauVirtuel.exe**

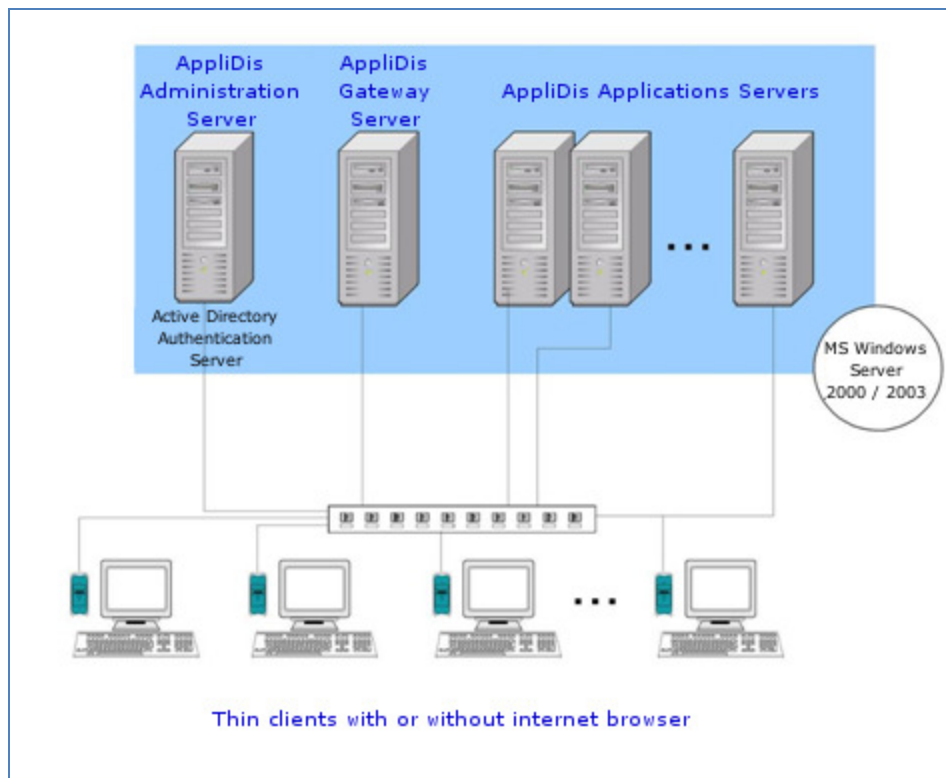


Figure 39 - Gateway and load balancing

Note: If you have set up redundancy of Administration servers and activated the virtual IP, deploy the Gateways on these two servers. Then configure your thin clients on this IP to profit from maximum continuity of service.

Gateway and protection of application servers

When your client workstations (regardless of their type – thin, light or fat clients) use the Internet to connect remotely to the Application servers, you can protect them in your private network. In this case external access is only authorized to the Gateway and AppliDis Administrator Servers. This solution protects your Application servers.

The configuration setting to install this solution is shown below:

1. Install a Gateway Server (see Installing a server p.85)
2. Check the Gateway option in the configuration menu and option sub-menu since in this case you will force all thin clients and all the other AppliDis clients (executed from the applications portal or Desktop mode) to connect to the Gateway
3. Then configure your thin client's Terminal Server client so that it connects to the Gateway device. To this end, launch the connection to the Gateway device (by using its name or its IP) on all the thin clients and enter the following start program: **BureauVirtuel.exe**

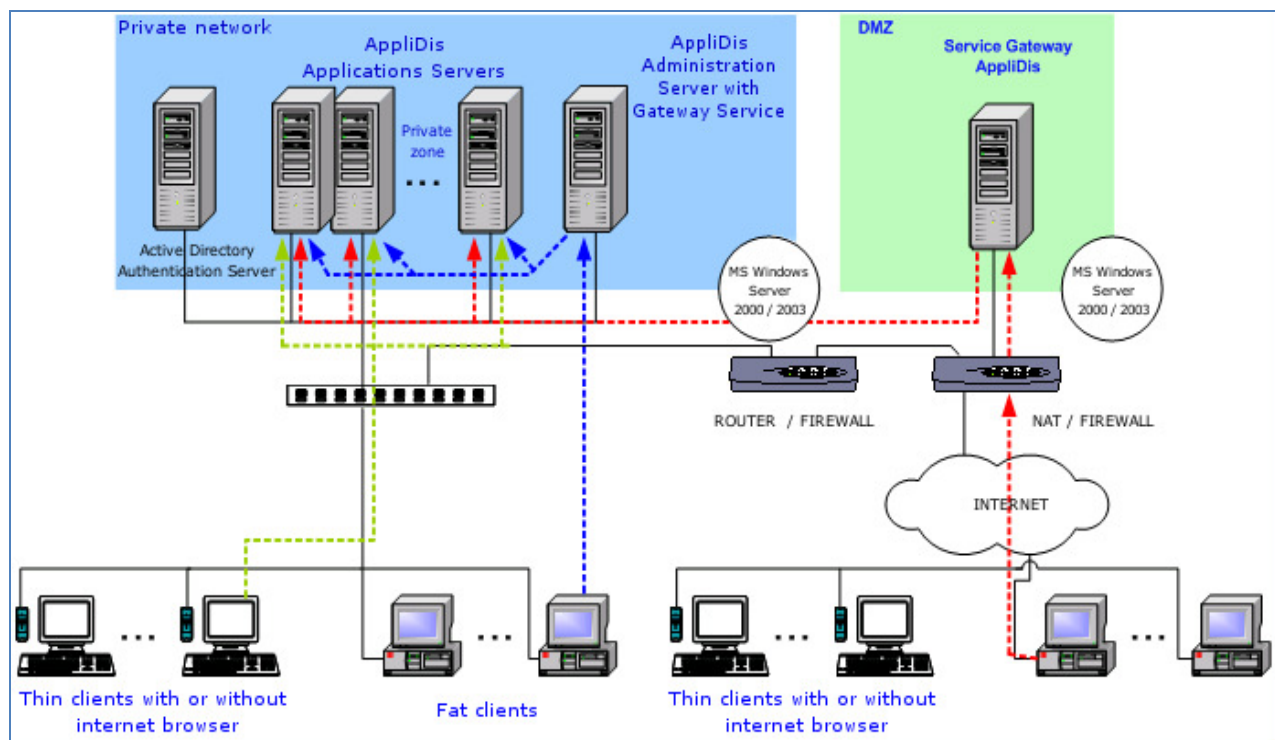


Figure 40 - Gateway and protection of application servers

Your firewall must be set so that the HTTP flow from the outside is redirected towards the Administration Server. With regard to the TCP/5300 router flow, this must be received on the Gateway device of your DMZ. The firewall separating the internal zone from the DMZ must also allow the Gateway located in the DMZ to communicate with each Application Server in TCP/3389 and the Administration Server in HTTP (TCP/80) or HTTPS. This configuration makes it possible to profit from load balancing from a public network towards a private network through, for example, an address translator.

Installing a server

An AppliDis server can be installed on the local device or on a remote device from the administration site. The list of devices that are suitable for installation comprises the Terminal Server devices in your domain. This list is generated in two different ways:

- Automatically: The list of suitable devices comprises all the active TSE servers specified by your domain controller.
- Manual: You can choose one of the machines listed by your domain controller: an exhaustive list of all machines, whether active or not.

Proceed as follows to deploy new servers:

1. Click on Servers in the main menu; by default you will be in the List of Servers sub-menu
2. Click on "Add automatically" or "Add manually" for the servers to build a list of suitable servers.
3. Only if you selected Add manually, create your list of suitable servers in the list on the right (select one or more devices from the computers in the domain and click on the ">" arrow, then click on Next).
4. The list of suitable devices will then be displayed. Select the device or devices on which you want to install an AppliDis Server, specifying the role - Application Server or Gateway Server - to be assigned (check box).
5. Then click on Install to install a server on these devices. Their state will change from "installation in progress" to "end of installation".

Checking server information

After installing an AppliDis Server, you can review its characteristics and modify some of them, such as the IP address (OS version of the Application Server or Gateway Server) or the connection port (Gateway Server).

1. Click on Server in the main menu; by default you will be in the List of Servers sub-menu
2. The list of registered servers will be displayed.
3. Click on the server whose characteristics you want to check (it will then be displayed enclosed in a red selection box)
4. The Properties button will be displayed. Click on this button.
5. A new page will be displayed with information which is accessed by clicking on the icons associated with the characteristics, TCP/IP addresses, connected group and operating system.

Setting the virtual IP address

Installing several AppliDis Administration servers guarantees maximum continuity of service. This redundancy is made possible by means of a virtual IP mechanism (IP Aliasing) managed by AppliDis.

This virtual IP address is carried by one of the Administration Servers. Should the server be unavailable, the virtual IP address will be carried by another AppliDis server which will take over automatically. The Administration Servers must be located in the same LAN. The virtual IP that you define must belong to the same IP network as your Administration Servers.

The administrator can select the period of time as from which a secondary Administration server must take over and become the main Administration server to compensate for the failure of the initial main server.

To configure the virtual IP address:

1. Click on Servers, then on the virtual IP Configuration sub-menu
2. This service can be activated or deactivated via the Activate check box
3. Enter the virtual IP address that you wish to assign to the master server, together with its subnet mask.
4. Regulate the Time interval between detecting the presence of the virtual IP address. This interval is 30 seconds by default.

Notes:

The virtual IP address can only be set for the Administration Servers.

When the administration site is accessed in order to change the configuration of the virtual IP, it is advisable to use the actual address or the name of the Administration Server in the Internet Explorer address bar, rather than the virtual address itself. This is because using the virtual address means you are likely to lose your connection to the administration site for a few seconds (the time it takes the virtual IP to be transferred from one Administration Server to another).

For your clients' convenience, it is recommended that you configure an entry in your DNS or WINS on this virtual IP so that your clients can access it by a name rather than an IP address.

Example:

Use the following address: <http://NomAdmin/AppliDis/Administration>

Instead of this: <http://10.11.12.13/AppliDis/Administration>

Modification of the IP address for a simple configuration

When an external access is to be created, a server must be able to have two IP addresses. The first, known as the "internal IP address" corresponds to the IP address used to access the server from a device in the Intranet network. The second, known as the "external IP address" corresponds to the address used to access the server via a router when accessing it from outside.

If a server has a specified internal IP address and an empty external IP address, the client will try to connect by the internal IP address only (the client performs a test to check that the specified IP address is indeed valid before beginning connection). This is in the event of a simple configuration, where for example all the client workstations are located on the same site in the same Intranet.

1. Click on Server in the main menu; by default you will be in the List of Servers sub-menu
2. The list of registered servers will be displayed.
3. Click on the server whose IP address you wish to modify.
4. Click on Properties.
5. Click on TCP/IP.
6. Change the Internal IP Address value then click on OK

Modification of the connection port for the Gateway Server

The Gateway Server listening and connection port is set by default to port 5300. This port can be modified:

1. Click on Server in the main menu; by default you will be in the List of Servers sub-menu
2. The list of registered servers will be displayed.
3. Click on the Gateway server whose connection port you wish to modify.
4. Click on Properties.
5. Click on TCP/IP.
6. Change the value of the Port then click on OK.

Setting the IP address for configuration with router

If, on the other hand, the server has a non-empty internal IP address and a non-empty external IP address, the client will test both addresses in parallel and keep the first for validation. In this case, the connection time is not increased because the test is carried out in parallel for both IP addresses.

To access this server via a router, a second IP address has to be set, corresponding to the address for this server as seen from the outside. Typically, this will be your router's external IP address.

1. Click on Server in the main menu; by default you will be in the List of Servers sub-menu
2. The list of registered servers will be displayed.
3. Click on the server whose IP address you wish to modify.
4. Click on Properties.
5. Click on TCP/IP.
6. Change the external IP address value then click on OK.

On your router or your firewall, you will need to authorize the opening of ports 80 (HTTP) and 3389 (RDP) from outside to inside. If the NAT function is active, port TCP/80 must point to the administrator and port TCP/3389 to port TCP/3389 on the Application server.

16.5 Activating the HTTP Gateway

From the Configuration/HTTP Gateway menu on the AppliDis Administration console, activate the Gateway function, then individually activate the AppliDis Administration servers which will run the service (First activate the Gateway Standard role on these servers, otherwise they will remain shaded out).

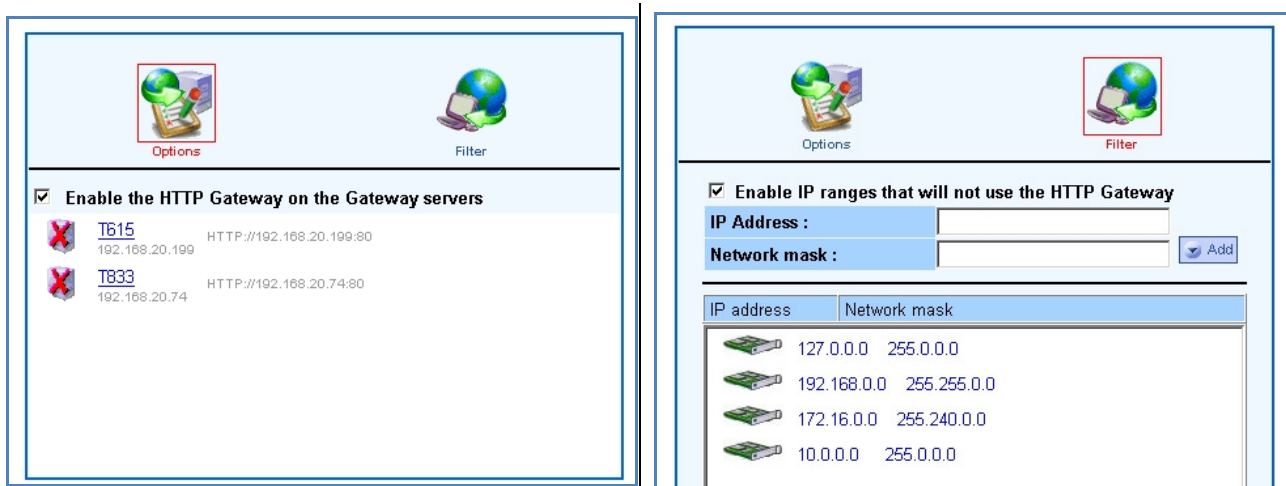


Figure 41 - Configuration of the Gateway access URL

Then configure the URL for access to the HTTP Gateway service for each server. The access URL is made up of the HTTP or HTTPS mode, the DNS name by which the clients will access the server (generally a DNS name corresponding to the firewall external IP) and then the service port (80 in HTTP mode or 443 in HTTPS mode).

1. In the Configuration menu, HTTP Gateway, check Activation of the HTTP Gateway.
2. Select the Administration Server which will be the HTTP server.
3. Check the server activation box.
4. Set HTTP or HTTPS mode.
5. Specify the DNS name through which the clients will come in.
6. The port must be specified (80 in HTTP or 443 HTTPS).
7. Click on OK.

Note: In HTTPS mode, your server must have a valid SSL certificate also corresponding to the DNS name of your access to the Gateway. SSL mode only functions if the 3 requirements set out below are satisfied:

- 1/ Common Name of the certificate equivalent to the DNS name specified in the interface (see Figure 19 Configuration of the URL for access to the Gateway).
- 2/ Certificate that is valid over time.
- 3/ Certificate approved by a root CA.

16.6 Configuring the settings of the Client zones using the HTTP Gateway

Depending on the origin of your clients, the HTTP Gateway may or may not have to be used. Generally, users of the LAN or users located in a WAN connected to the servers by VPN are not affected by this configuration setting since they can communicate directly with the application servers. External users, however, pass via the HTTP Gateway. AppliDis enables you to accurately define the IP ranges for which the direct mode will be used. In the Configuration/HTTP Gateway menu, select the filtering menu. Specify the IP ranges for which the HTTP Gateway will not be used.

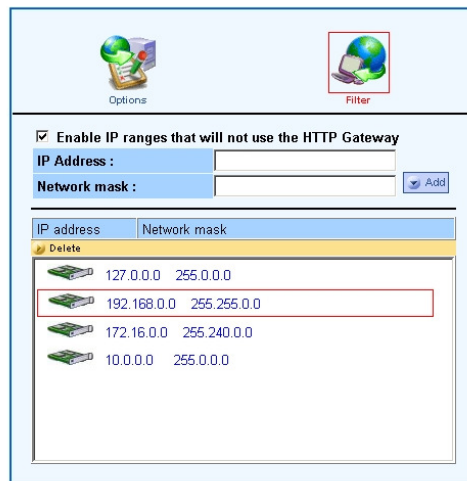


Figure 42 - IP range of clients not using the HTTP Gateway

Note: The client IP that is taken into account is the one provided by the IIS platform. Thus, for any client located behind a NAT, the IP perceived by IIS is generally the public IP of the NAT and not the client's actual internal address. The default settings are shown in the table below:

Table 1 Private IP ranges

Network address	Mask
127.0.0.0	255.0.0.0
192.168.0.0	255.255.0.0
10.0.0.0	255.255.0.0
172.16.0.0	255.240.0.0

Uninstalling a server

Uninstalling a server makes it inactive in AppliDis. It removes all the AppliDis files installed on this server.

1. Click on Server in the main menu; by default you will be in the List of Servers sub-menu.
2. The list of devices hosting a server (application or gateway server) will be displayed. Select the device on which you want to uninstall an AppliDis Server (this device will then be displayed framed in red).
3. Click on Remove in order to uninstall the AppliDis server.
4. A removal confirmation window will be displayed. Click on OK.
5. You can follow the uninstallation of the server by means of feedback messages: removal of server in progress at the time of the action of removal and End of removal of server when the removal has been completed.

Note: A server which has the role of Administration server cannot be removed from the AppliDis console. To uninstall this role, the Windows Add/Remove Programs menu must be used.

16.7 Creating and removing server groups

Server groups make it possible to group several AppliDis servers together within the same entity. Special privileges can then be set on a server group rather than on a single server.

These groups can also be used to manage server farms on different sites by means of a "client workstation/server group" connection

Creating a server group

With AppliDis, your AppliDis servers can be grouped into server groups. These server groups can be used to configure access privileges to your AppliDis users, by server group (cf. "Access privileges on server", on page 127).

Example: creating an "office server" group composed of servers on which office applications will be available.

1. Click on Server in the main menu.
2. Click on the Server Groups sub-menu
3. A new page will open. Click on the New group button
4. Enter the name of the server group which you want to create, then click OK.
5. To add a server to the group. Go to the List of servers sub-menu
6. Click on one of the servers so that it is framed in a red selection box.
7. The Properties button will be displayed. Click on this button.
8. A new page will be displayed with information that can be accessed by clicking the corresponding icons. Click on Connected Group.
9. In the list of server group names, select the name of the group in which you want to place the server. Then click on OK.

Removing a server group

Removing a server group does not remove the servers belonging to this group from AppliDis.

1. Click on Servers in the main menu. By default, you will be in the List of Servers sub-menu
2. Click on the Server Group sub-menu
3. Click on the server group which you want to remove. This will then be framed in red.
4. Select Remove.

Note: when a group is removed, the servers contained in the group return to the Default group.

16.8 Applications on application servers

Applications are installed on each application server. This chapter describes the management and installation of the applications on the servers. However, all the applications present can be listed for a given application server.

Listing of applications available on an application server

When an Applications Server is installed on a machine, it will regularly send the Administration Server a list of applications running on the machine. This action is called "automatic application referencing". You can then consult a list of the applications registered on all AppliDis servers (see "

Management of client desktops" under the section "**Checking the automatic recording of an application**" on page 101).

1. Click on Server in the main menu; by default you will be in the List of Servers sub-menu
2. The list of registered servers will be displayed.
3. Click on the server whose list of recorded applications you wish to review (this will then be framed by a red selection box)
4. The Applications button will be displayed. Click on this button.
5. A new page will be displayed with the list of applications recorded for this server.
6. When you have finished reviewing the list of applications, just click on Back.

16.9 Monitoring and maintenance of servers

It is possible to monitor the use of AppliDis servers which enables you to analyse trends in order to program maintenance at a convenient time.

Listing the applications in progress and the users connected to a server

These functions, available for each server, will provide access to the Dashboard (for further explanations, please refer to "

Using the ", page 129).

1. Click on Server in the main menu; by default you will be in the List of Servers sub-menu.
2. Select the server for which you wish to carry out an action.
3. Click on Connected Users or Applications in progress to return to the Dashboard for this server.

Accessing a server via Microsoft "Terminal Services"

If you wish to carry out maintenance on a particular server which requires a connection with "Terminal Services", this can be done directly from the administration console.

1. Click on Server in the main menu; by default you will be in the List of Servers sub-menu.
2. Select the server on which you wish to connect.
3. Click on Access.
4. Connection is then possible in Full screen mode or in Included in page mode; the connection is automatically made as soon as the desired mode has been selected.
5. When you have finished managing your server remotely, just close the Terminal Server session (using the start button in the Terminal Server session) and your Internet browser will display the AppliDis servers page again

17 Management of client desktops

The client workstation management menu allows the maximum adjustment of effective configuration settings on the desktops of users of the AppliDis thin desktop. In this way, the behaviour of the users' work environment can be modified very quickly.

17.1 Placing icons on the user's desktop

The option "Place icons on the desktop" makes it possible to activate the automatic placement of the AppliDis application icons on the thin desktop.

1. Click on the Client desktops menu in the main menu; by default you will be in the Virtual desktops / options sub-menu.
2. Check the 'Place the icons of the published applications on the virtual desktop' box.

17.2 Application security

The "Name of executable" option makes it possible to define a list of authorized or prohibited executables directly or indirectly on start-up by the user. For example, if IEXPLORE is denied permission to start, the user will not be able to display Web pages, even from an application that opens the application automatically.

1. Click on the Desktops menu in the main menu; by default you will be in the Virtual desktops / options sub-menu.
2. Click on the Application security icon.
3. Specify the name of the executable either by entering it, or by using the Browse button.
4. Click the Add button.
5. Validate your additions by pressing the OK button.

17.3 Management of file extensions

The "Extension security" option makes it possible to specify authorized or prohibited extensions.

1. Click on the Client desktops menu in the main menu; by default you will be in the Virtual desktops / options sub-menu.
2. Click on the Extension security sub-menu.
3. Select the unauthorized extensions from the list of extensions proposed.
4. Press the OK button to validate your selection.
5. Note: You can also enter new extensions by entering them and pressing on the Add button. The OK button must then be pressed to validate your selection.

Note:

- 1/ if an application is present in a contract and at the same time barred from execution, it cannot be launched by users.
 - 2/ If a file type is access barred and if the application corresponding to this file type is placed in a contract, users with access to the contract and thus to the application will be able to access and launch the prohibited file type.
-

17.4 Connections

In the "Client desktops" menu in the AppliDis Administration console, a "Connections" sub-menu makes it possible to manage client desktops according to their IP address ranges, in order to connect them to a server farm.

Depending on your configuration settings, the user will be directed by load balancing onto a server of the farm to which it is connected. If no server in its farm is able to respond, it will then be sent to the first available server of any farm.

This function is activated via the Configuration/Options menu of the AppliDis Administration console. The "Connecting client workstations/Server groups" box has to be checked in order to do this.

Connection tab

The "Connections" interface enables you to assign a server group to each IP zone of your client workstations.

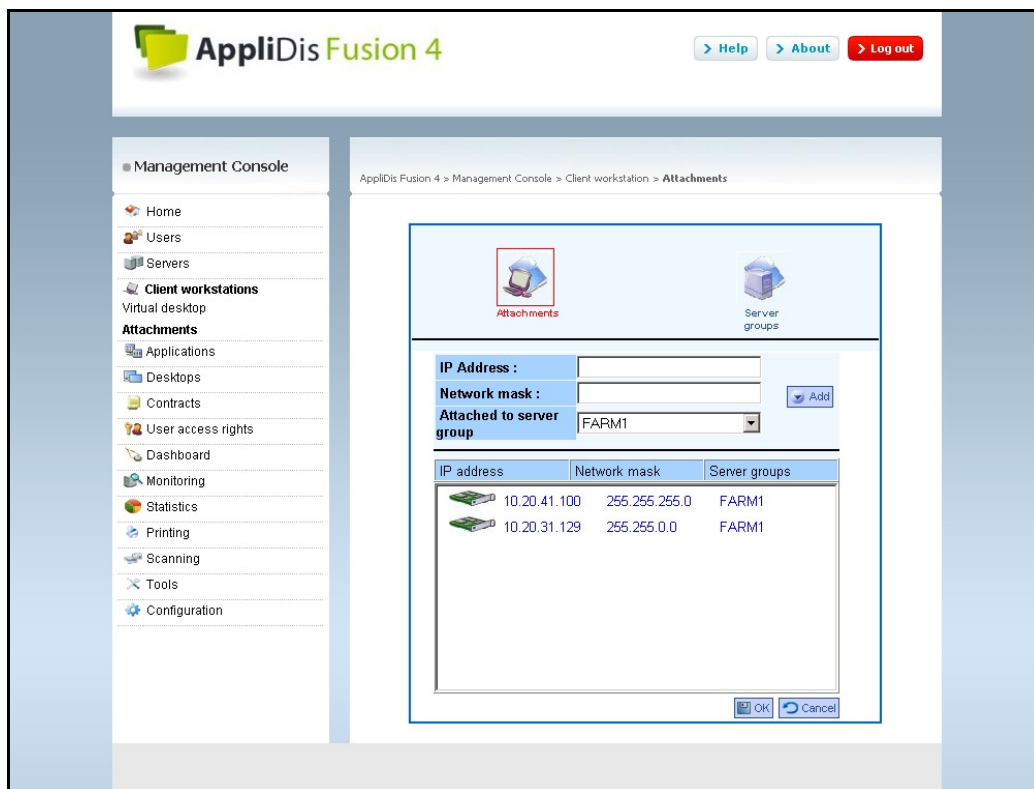


Figure 43 - Connections to server group

Specify the various zones (or network maps) for which you wish to assign a server group, then click on the Add button. The configuration settings located at the top of the list have priority. When a zone is located in the list, you can select it and then raise or lower its priority by using the Up / Down button when you select a line.

Server Groups tab

This page enables you to automatically switch the whole selection of servers onto a server group.

Select a server to be added to the group and click on the arrow pointing right to move it from the list on the left to the list on the right. You can repeat this operation several times in order to move all the servers you want to be assigned to the server group into the list on the right.

You can also decide to assign all servers by clicking on the double arrow pointing right.

Click on OK and your server group will be filled with the selected servers.

You can also remove a server from the server group by selecting it from the list on the left and clicking on the Remove button. Click on the Remove All button to remove all the connected servers of this group.

When a server is removed from a group, it returns to the "Default" group.

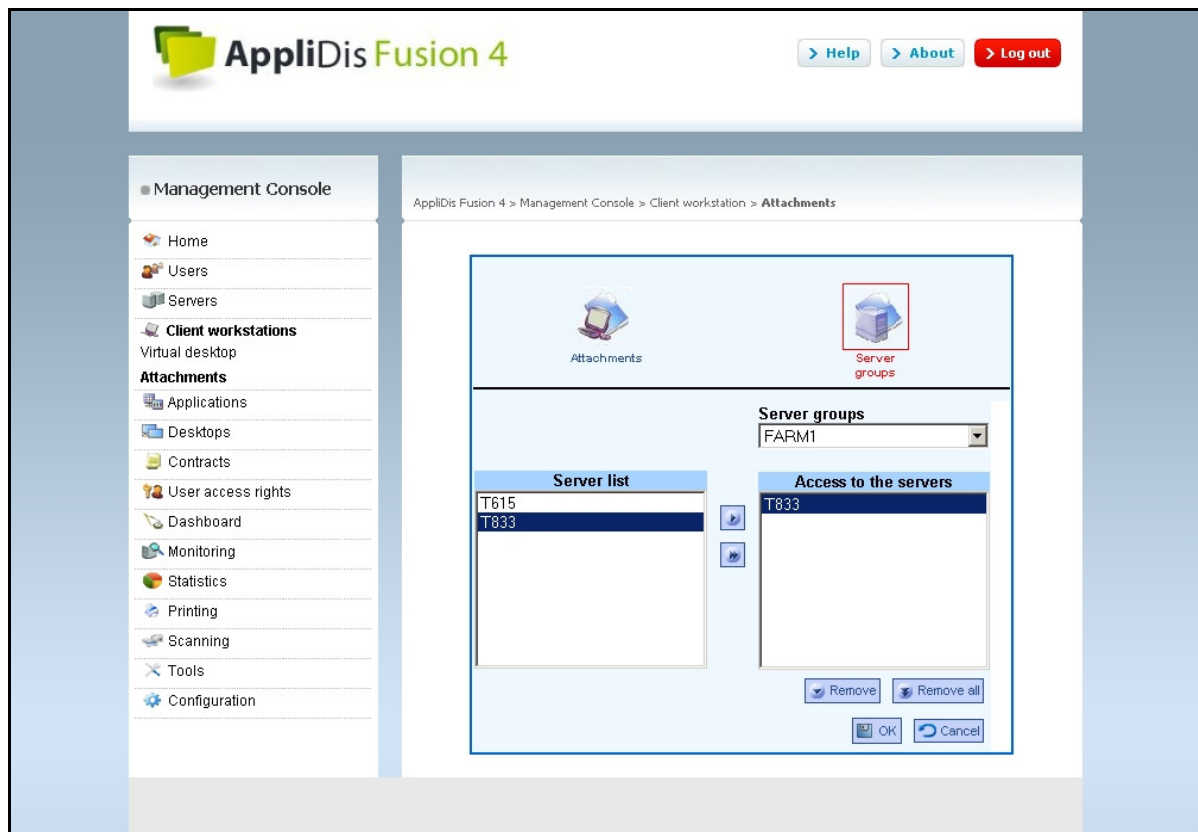


Figure 44 - Removing a server from a group

18 MyApps Catalogue

The AppliDis MyApps catalogue allows users to request access to one or more applications placed by the administrator in the AppliDis MyApps catalogue. It is then up to the administrator to approve or deny the user's request. If the user's request is approved, the application will appear along with the other applications to which he/she already has access privileges.

Furthermore, a comments and scoring area is available for applications, enabling users to review applications in order to assist other users in choosing which new applications to use.

18.1 Configuration

To activate AppliDis MyApps, check the "MyApps application catalogue" box in the "Configuration/General Options" menu. The "MyApps Catalogue" appears in the administration console and the user portal.

18.2 Application access request

This is the default page when going to the MyApps Catalogue menu. This is the application access requests management page. This page enables the administrator to manage requests generated by users regarding access to applications which they have found in the AppliDis MyApps catalogue.

The administrator views the status of the request (Request posted, being processed, granted or denied), and may grant or deny requests or mark them for processing.

The display of requests may be filtered and sorted by application name, user, date and request status.

When an application access request is granted, a contract is created between an AppliDis group consisting only of the user in question and the application, with the option of creating an instance. This group is called "grp_public_USRNAME", where USRNAME is the AppliDis name of the user in question.

When a request is refused or marked for processing, any pre-existing contract for the user in question is simply removed.

Search

By default, selection is made on the basis of the status settings "Posted" and "In Progress".

If a search is performed while selecting an application name, a user name or a date with a blank text field, no filter is applied to these settings.

Caution: When selecting an application name or user name, the text field must exactly match a precise name in the database. There are no options for entering a partial word or adding a wildcard character such as * for the remainder of the word.

The Result:

When a user makes an application access request, the request is automatically assigned "In Progress" status.

When an "In Progress" application is selected, it may either be granted or denied.

When a granted application is selected, it may either be refused or reset to "in progress" status.

When a status is changed from "in progress" to "granted" or "denied", an email is sent to the user notifying them of the change of status.

A sort is performed, by date as default. Sorts may be made by status, application, user or date.

18.3 Management of Public Applications

To add an application to the public catalogue, a button appears in the list of applications once the AppliDis MyAppS application catalogue has been activated in the "Configuration/General Options" menu. Once the administrator has chosen an application and clicked on this button, the application will automatically be added to the public catalogue after confirmation.

On the "Public Applications Management" page, the administrator can view and manage applications which are available in the public catalogue.

The administrator can disconnect an application from the catalogue. The consequence of this is that the application will no longer be visible in the user catalogue, although users previously granted access privileges will continue to have access to the application.

The administrator can view the properties of the application.

18.4 Management of access to the catalogue

This screen manages users' access to the catalogue. If a user does not have access to the catalogue, the Catalogue menu will remain empty.

The administrator can select groups or OUs which will have access to the catalogue by moving them to the right of the screen; or vice versa, if the administrator wants users not to have access to the catalogue.

Removing access to the catalogue for a group does not automatically remove access to applications which have been authorised for members of this group.

19 Application management

19.1 List of applications

An ordered list is available which shows all the installed applications. This list displays all the applications referenced by AppliDis as well as manually deployed applications. These applications can be filtered according to the following criteria:

- **Group:** displays only the applications present in this group.
- **Referenced today:** displays only the applications referenced today, which is useful when you wish to configure newly installed applications.
- **Priority:** displays only the applications for the selected priority.
- **Display the applications referenced in the Start menu:** activating this box masks all the applications not referenced in the server Start menu.
- **Mask system applications:** hides applications in the system folders of your Applications Server.
- **Mask console applications:** hides applications running in console mode.

19.2 Principle of application referencing

A major advantage of AppliDis is that it enables the administrator to reference applications on the AppliDis servers without having to carry out any particular actions in most cases. There is an automatic referencing system which is based on the recognition of user applications currently being executed on the servers. For example, simply running an application such as "Notepad" allows that application to be automatically referenced in AppliDis.

The automatically referenced application is by default assigned the name of its executable minus its extension (for example the Microsoft Word application will be recorded automatically in AppliDis under the name 'WinWord' because the name of its executable is winword.exe).

As part of this automatic referencing, the version of the executable is also recorded by AppliDis.

If you have several AppliDis Application Servers, you will no doubt wish to use the load balancing feature, see "

Several servers with load balancing" page 50. You will then have the same application located on several servers. During automatic referencing, AppliDis will try to create a single application, but will assign several locations for it. In order to obtain multiple locations for the same application, the following conditions must be satisfied:

- The application must be executed at least once on each server
- The executable must have the same version number. More specifically, only the major version number needs to be the same. The major number is the first figure of the version number (i.e., if the version is "5.2.1.6", the major number is 5)

Textbook case

If an application is only referenced on a server A with the path "C:\path1\executable name.exe", and the same executable with the same version is detected on a server B with the path "C:\path2\executable name.exe" (in our case, path2 can be the same as or different from path1), a new application is not created, just a new path for the application which already exists. AppliDis thus tries to associate identical executables located on several servers if they have the same version.

If an application is recorded on two servers A and B with the respective paths "C:\path1\executable name.exe" and "C:\path2\executable name.exe", and the same executable with the same version is detected for the second time on server B with the path "C:\path3\executable name.exe", a new application is created which is only available on server B with the path "C:\path3\executable name.exe". AppliDis creates a new application when a different path already exists for the same device.

If the same application (with the same version number) is detected several times on the same server with different executable paths, AppliDis will create this application several times by adding a "#1", "#2", etc... at the end of each application name in order to differentiate between them.

19.3 Advanced referencing of applications

When using several AppliDis Application Servers in load balancing, the applications must be referenced for each application server. You can simply reference your applications on a single server and copy the configuration settings of applications executed on one server to all the other servers. Thus, the administrator can configure applications on a particular server which will be used as a reference server. All these configuration settings can be copied onto a set of servers with just a few mouse clicks. A report is generated so that operations can be audited to ensure they are carried out correctly. Should an application not be installed on a server, the application will be referenced in a "deactivated" status.

To use advance referencing:

1. Click on Applications in the main menu, then on Advance Publication.
2. Select the reference server, then Next.
3. Select the applications to be referenced in the list on the left, then Next.
4. Select the servers on which the application will be referenced, then Next.
5. AppliDis will check for the presence of these applications on the selected servers. The progress bar will indicate the progress of the operation. A report will be generated and displayed at the end of the procedure. In the event of an error, the applications involved will be marked "deactivated" in AppliDis.

The displayed report is stored in an installation directory at the following location on the AppliDis Administration server: **%APPLIDIS%\LogFiles\Rapports.**

Notes: This referencing operation can be carried out as many times as necessary. If you notice that an application is not installed on a server at the time of this operation, you can repeat this referencing step after the application has been installed. If successful, the location of the application that was previously deactivated will be activated and will be fully operational.

Checking the automatic recording of an application

1. Click on Applications in the main menu.
2. The list of all the applications classified in alphabetical order will then be displayed. If the number of applications is high enough to display the classification of applications by letters, and if you know the name of the executable program of your application, click on the first letter of the program name (for example "w" for WinWord) to go directly to the page containing your application.

Renaming an application

Whether the application is referenced automatically or manually, its settings can be modified. Under automatic referencing, it may be useful to rename the application (for example replacing "Winword" with "Word XP").

1. Click on Applications in the main menu.
2. Select the application whose name you wish to modify by clicking on its name in the list
3. Click on Properties.
4. In the 'Name displayed for the application' field, enter the name which you wish to give to this application.
5. Click on OK.

Note: When an application is automatically registered, by default it is registered in the 'APPLICATION' mode. This mode is explained in paragraph "Normal mode or application mode for applications" p.112

19.4 List of available servers to an application

This function makes it possible to review the various AppliDis servers where a given application is available. This enables you to see, for example, that the application "Word" is available on the server "server1" whereas the application "Excel" is available on the servers "server1" and "server2".

1. Click on Applications in the main menu.
2. Select the application for which you wish to see the available servers. It will be displayed framed in red.
3. Click on Properties.
4. In the application properties, click on Location. The various servers on which the application is installed will be displayed

19.5 Manual referencing of an application

Referencing of an application in AppliDis is done manually when the application has not yet been recorded in AppliDis (in this case, an 'add applications' wizard will be displayed in three stages where the name, executable path and membership groups can be set). For example, if the Notepad application is not yet included in the list of the applications, you can add it by setting the name displayed as "Notepad" and the path as "C:\winnt\system32\notepad.exe" on the server "Server1", entering it in an application group called "Office apps". You will find more information under the heading "Adding a new application"

Adding a new application

A new application can be added with the help of a wizard which divides the task into three stages. For each stage, the corresponding icon will be displayed in color while the other two will be shaded out.

1. Click on Applications in the main menu. By default, you will be in the "List of applications" sub-menu.
2. Click on New application
3. In the 'Name displayed for the application' field, enter the name that you wish to give to this application. You can also define a description of the application, a work directory and a line of settings to give to the executable
4. Then choose its mode: Normal or Application, see "

Normal mode or application mode for applications" page 112 (step 1)

5. Click on Next to go on to step 2.
6. In order to fill the Path field (step 2), select a server then click on Browse.
7. A window will open; select the disk and the path of the application. When you have found the required executable, double-click on it.
8. You will then be returned to the first screen.
9. Click on Next to go on to step 3.
10. Select the application groups to which the application will belong by displaying these groups in the list on the right by means of the right arrow (step 3).
11. Click on OK to save this new application.

19.6 Add an application to the MyApps catalogue

Once an application has been referenced in AppliDis Fusion 4, it is possible to add it to the MyApps catalogue. To do so, click on the application, and click on the "Add to catalogue" button. The application will automatically appear in the list of available applications in the catalogue.

To find out more about how the AppliDis MyApps catalogue works, see paragraph " MyApps Catalogue" on page 97.

19.7 Advanced properties of an application

It is also possible to modify other settings for each application such as responsiveness, the resolution or the level of priority of the application.

Modifying the responsiveness of an application

This concerns the responsiveness of the mouse during the use of the application. This setting is particularly useful for certain CAD software which requires highly accurate mouse work. The default value (100) is not satisfactory in this case, and a value of "10" will provide you with greater cursor flexibility for the application.

1. Click on Applications in the main menu. By default, you will be in the "List of applications" sub-menu.
2. Click on the application which you want to make available for a server (it will then be surrounded by a red box)
3. Click on Properties.
4. The general information is displayed by default. Click on Advanced Settings.
5. The default value is 100 ms for Application response time; select the desired value from the list
6. Click on OK.

Note: Changing the responsiveness of an application impacts on the volume of information exchanged between the client workstation and the AppliDis server. A value lower than 100 (default value) will involve greater usage at network level. Care should be taken when modifying this setting.

Modifying the screen resolution of the application

The resolution of a session can be modified by selecting a pre-set value or by choosing full screen mode. The application will then be launched in a session which will temporarily replace the desktop of your client workstation.

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application for which you wish to modify the screen resolution (it will then be surrounded by a red box)
3. Click on Properties.
4. The general information is displayed by default. Click on Advanced Settings.
5. The default value is Client Resolution for Application screen resolution; select the desired value from the list
6. Click on OK.

Modifying the priority of an application

This relates to the CPU time given to the application. The higher the application's priority, the more CPU time it is likely to be allocated. It will therefore have an advantage over other applications in the event of heavy CPU loads on the server. For more information, see "Application priority levels", p. 111.

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application for which you wish to modify the priority (it will then be surrounded by a red box).
3. Click on Properties.
4. The general information is displayed by default. Click on Advanced Settings.
5. The default level of priority is Normal priority. To increase its priority, select High or critical priority, to reduce it select Low or very low priority
6. Click on OK.

Modifying limits on instances per user

You can limit the number of times an application can be launched per user. For example, it is not necessary to authorize a user to be able to launch several instances of OUTLOOK.

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application for which you wish to modify the priority (it will then be surrounded by a red box).
3. Click on Properties.
4. The general information is displayed by default. Click on Advanced Settings.
5. By default, the number of instances per user is unlimited. You can select a number of instances between 1 and 5 per user.
6. Click on OK

19.8 Adding / Activating / deactivating a location for an application

If two AppliDis servers are used, load distribution (where the server most suitable to execute the application is calculated in real time) is carried out if the application is recorded on several servers. The load distribution function finds the best server from the various locations of the application. If you wish to launch an application on a particular device, it is thus advisable to deactivate the locations of the application on the other devices. In the same way, if you wish to prevent the launching of an application on a specific device, just deactivate the location on this device.

A location for an application is created during the process of referencing the application. See also paragraph "

Adding a **new application**", p 102.

Note: In order to prevent the launching of an application from a specific server you may be tempted to remove the location from this server. However, this solution is not recommended since the automatic referencing of applications could add the removed location again if the application is executed for a few moments on this server. It is recommended that you deactivate the location

Adding a new location for an existing application

This option makes it possible to manually reference an application that is already recorded on one Application Server on another Application Server where it is not defined as available.

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application which you want to make available for a new server (it will then be surrounded by a red box)
3. Click on Properties.
4. The general information is displayed by default. Click on Location.
5. A page will open with all the servers on which the application is available
6. Click on New location
7. The window will then display two fields to be filled in: the name of the server on which you want to add the application and the path to the executable on this server.
8. Click on Browse to look for the executable. A new window will open: select the disk and browse through the directories until you find the executable. Double-click on the executable.
9. You will be returned to the first window, where the new server and the path of the executable previously selected will be displayed.
10. Click on OK to add this new location for the selected application.
11. The application will now be available on the server which you have just specified.

Activating a location for an application

Activating an application location on a server makes this server suitable for application launching (load balancing) by a user if this user has privileges to access this server.

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application for which you want to activate a location (it will then be surrounded by a red box).
3. Click on Properties.
4. The general information is displayed by default. Click on Location.
5. A page will open with all the servers on which the application is available.
6. Select the server on which you want to reactivate the application. The name of the server and the path to the executable will be framed in red.
7. Click on Activate.

Deactivating an application location

Deactivating an application location on a server prevents this application being executed on this server via AppliDis.

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application for which you want to deactivate a location (it will then be surrounded by a red box).
3. Click on Properties.
4. The general information is displayed by default. Click on Location.
5. A page will open with all the servers on which the application is available.
6. Select the server on which you want to deactivate the application. The name of the server and the path to the executable will be framed in red.
7. Click on Deactivate.

19.9 Removing an application or removing an application location

Removing an application location is necessary when the application is uninstalled from one of the AppliDis servers. Take, for example, the application "Word" present on two AppliDis servers "server1" and "server2". It has a contract and is referenced on both servers. When the user executes this application via AppliDis, this application will be executed on one of the two servers by means of load distribution. If the application is uninstalled from "server1", the load balancing function must not be able to select "server1" as a possible server any more. The location must therefore be removed from the server "server1".

Conversely, it may be necessary to remove an AppliDis application in order to clean out the stock of applications recorded in AppliDis. However, it should be remembered that the automatic referencing of applications will record the application in AppliDis again if it is executed again on an AppliDis Server after it has been removed. Removing applications thus applies mainly to applications which will no longer be executed on any of the AppliDis servers (for example, applications that are uninstalled definitively from the AppliDis servers).

Removing an application

The application should not have any contracts on it.

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application which you want to remove.
3. Click on Remove.

Removing an application location

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application for which you want to remove a location on a server (it will then be surrounded by a red box).
3. Click on Properties.
4. The general information is displayed by default. Click on Location.
5. A page will open with all the servers on which the application is available.
6. Select the server on which you want to remove the application location. The name of the server and the path to the executable will be framed in red.
7. Click on Remove.

19.10 Creating and removing application groups

Application groups make it possible to group together the applications recorded in AppliDis by topic. For example a group called "Office apps" can be created from AppliDis applications such as, "Word", "Excel" and "PowerPoint". This group structure will then be displayed twice: firstly in the presentation of the applications on the applications portal (the applications are classified by groups) and secondly at contract level (for more information, please refer to the contract management section).

Creating an application group

Application groups are created with the help of a wizard, which divides the task into two stages: first the name of the group, then the applications that this group will contain.

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the Application group sub-menu.
3. Click on New group.
4. Enter the name of the group (step 1).
5. Click on Next.
6. A page will open with two lists (step 2): the list on the left displays all the applications available in AppliDis, while the list on the right displays all the applications assigned to this application group.
7. Select an application to be added to the group and click on the arrow pointing right to move it from the list on the left to the list on the right. You can repeat this operation several times in order to move all the applications to be assigned to the application group into the list on the right.
8. You can also decide to assign all the applications by clicking on the double arrow pointing right.
9. Click on OK and your application group will be created and filled with the selected applications.

Removing an application group

Removing an application group does not remove the applications which it contains. Moreover, an application group cannot be removed if a contract is placed on this application group. In this case the contract must first be removed before the application group can be removed.

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the Application group sub-menu.
3. Click on the application group which you want to remove. This will then be framed in red.
4. Select Remove.

19.11 Assigning relationships between applications and application groups

Relationships between application groups and applications can be defined in the two following ways:

- In the properties of an application, set the membership groups for this application
- In the properties of an application group, set the applications which it contains.

To add application groups to a given application

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application for which you want to add application groups.
3. Click on Properties.
4. The general information is displayed by default. Click on Groups.
5. A page will open with two lists: the list on the left displays all the application groups available in AppliDis, while the list on the right displays all the application groups assigned to this application.
6. Select a group to be added to the application and click on the arrow pointing right to move it from the list on the left to the list on the right. You can repeat this operation several times in order to move several groups assigned to the application into the list on the right.
7. You can also decide to assign all the groups to the application by clicking on the double arrow pointing right.
8. Click on OK.

Removing application groups from a given application

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application for which you want to remove application groups.
3. Click on Properties.
4. The general information is displayed by default. Click on Groups.
5. A page will open with two lists: the list on the left displays all the application groups available in AppliDis, while the list on the right displays all the application groups assigned to this application.
6. Select a group to be removed from the application (list on the right) and click on Remove. You can repeat this operation several times in order to remove several groups.
7. You can also decide to remove all the groups from the application by clicking on Remove all.
8. Click on OK.

Adding applications to a given application group

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the Application group sub-menu.
3. Click on the application group for which you want to add applications.
4. Click on Properties.
5. The general information is displayed by default. Click on Applications.
6. A page will open with two lists: the list on the left displays all the applications available in AppliDis, while the list on the right displays all the applications assigned to this application group.
7. Select an application to be added to the group and click on the arrow pointing right to move it from the list on the left to the list on the right. You can repeat this operation several times in order to move all the applications to be assigned to the application group into the list on the right.
8. You can also decide to assign all the applications by clicking on the double arrow pointing right.
9. Click on OK.

Removing applications from a given application group

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the Application group sub-menu.
3. Click on the application group for which you want to remove applications.
4. Click on Properties.
5. The general information is displayed by default. Click on Applications.
6. A page will open with two lists: the list on the left displays all the applications available in AppliDis, while the list on the right displays the applications assigned to this group.
7. Select an application to be removed from the group (list on the right) and click Remove. You can repeat this operation several times in order to remove several applications.
8. You can also decide to remove all applications by clicking on Remove All.
9. Click on OK.

19.12 Application priority levels

Applications have several levels of priority which allocate them more or less CPU time on the server. Applications with a high level of priority are thus favored in the event of server CPU overload, and are thus more flexible. The levels of priority are (in ascending order): very low, low, normal, high, critical. By default, applications recorded in AppliDis (automatically or manually) have a 'normal' level of priority.

Note: For the levels of priority to be taken into account, the corresponding AppliDis module must also be activated cf "Application priorit" p.184.

Displaying application priority

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. You can display the application's priority by clicking on Display priorities.
3. The application priorities will then be displayed in red boxes located under the application. One red box corresponds to a "very low" priority and five red boxes to "critical" priority.

Sorting applications according to their priority

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. You can then select Sort the applications by priority by clicking on Priority and by choosing the desired category from Very low priority to Critical priority.

Managing priority groups

You can assign the priority of one or more applications at the same time.

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the Application priority sub-menu.
3. Select the priority for which you want to add or remove applications from the drop-down list.
4. The list on the left will display all the applications recorded in AppliDis, while the list on the right will display those that already have this level of priority.
5. Click on one or more applications in the list on the left, then click on the arrow pointing right to move them into the list on the right.
6. Click on OK.

19.13 Normal mode or application mode for applications

The two modes are different from the point of view of presentation and consumed resources.

Presentation

In **normal** mode, the application required by the client is displayed in a window called AppliDis Client. There are thus as many AppliDis Client windows as there are applications executed by AppliDis. In **application** mode, there is no way of differentiating between applications executed remotely and those executed locally: the user will thus see his application executed remotely without a distinctive sign of an application executed on his device.

Resources used

In normal mode, each application required by the client has a corresponding Terminal Server session open on the server. There may thus be a large number of sessions open on the server for the same user. In application mode, the user opens a first session on the server when the first application is launched. Each time an application is launched, it will be executed in this session. This reduces the usage of server resources and reduces the time needed to open the application required by the user.

When load balancing is used, see "

Several servers with load balancing" page 50, a second application is launched in a session that is already open if the most suitable server is still the same server that was selected for the first application. Conversely, if the most suitable server selected by the load balancing function has changed, the session will be opened on this new most suitable server. In the latter case, if a third application is opened, it may be executed directly in the session already open on either of the two servers used.

Configuring the application mode

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application for which you want to configure the mode (it will then be surrounded by a red box)
3. Click on Properties.
4. In the Execution mode line, select normal mode or application mode.
5. Select OK to save your modifications

19.14 Selecting the application icon

By default, AppliDis places the first icon in the internal resources of the binary file you select. Some binary files may not contain icon resources, in which case AppliDis will select an icon by default. You can select a new icon for your application by modifying the properties of the application. This icon can be selected from the following file types:

- **Executable file:** A .EXE file can contain an indefinite number of icons. The list of icons contained in a binary file is displayed by selecting the file. If no icons are present, a "no icon" message will be displayed.
- **Library file:** A .DLL file can contain any number of icons. The list of icons contained in a DLL is displayed by selecting the DLL. If no icons are present, a "no icon" message will be displayed.

Modify icon

1. Click on Applications in the main menu. By default, you will be in the List of applications sub-menu.
2. Click on the application for which you wish to modify the icon (it will then be surrounded by a red box)
3. Click on Properties.
4. Click on the Change button
5. Using the browser interface, select the resource file containing the desired icon.
6. Select the icon (it will then be surrounded by a red box)
7. Click on the Select this icon button
8. Click on OK to save the changes

20 Desktop management

20.1 List of desktops

The list of desktops displays the available desktop pools. This list contains all the desktop pools created by the administrator in AppliDis.

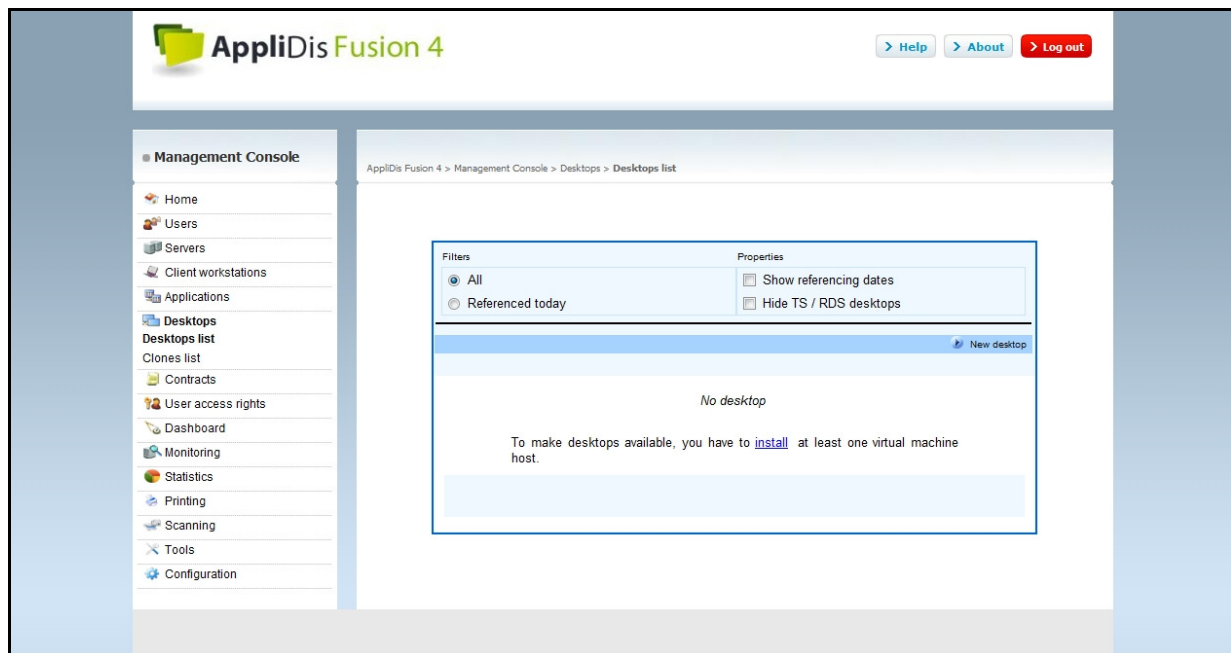


Figure 45 - Desktop list

By default, if you have at least one application host server and Windows desktop server, you will automatically have an RDPDesktop desktop in this list.

These desktops can be filtered according to the following criteria:

- **All:** displays all existing desktops
- **Created today:** Displays only desktops created today, which is useful if working on newly-created desktops.

In addition, you can show the desktop creation date by checking the "Display creation date" checkbox.

You can hide the RDPDesktop desktops from this list by checking the "Mask RDPDesktop" box.

Creating a desktop (or collection of desktops)

Apart from TS / RDS desktops, which are created automatically when the first applications host server and Windows desktop server is added, desktops (or collections of desktops) must be created manually.

New desktops are added via an assistant, which breaks the task down into four stages. For each stage, the corresponding icon will be displayed in color while the other two will be shaded out.

1. Click on "Desktops" in the main menu. By default, you will be in the Desktops sub-menu.
2. Click on the "New Desktop" button
3. In the "Name" field, which is compulsory, enter the name you wish to give this desktop.
Caution: this field is limited to 8 characters. You can also assign a description to a

desktop, then specify the action to be performed when the user disconnects. 3 choices are possible:

- a. Restart and pause the machine (default value)
- b. Halt the virtual machine
- c. Restart the virtual machine

4. On the following screen, you must choose the location of the virtual images. To do so, click the "New location" button. In the Host area, select the hypervisor which will host the reference virtual desktop clones.
5. Next, choose the reference machine to be cloned and made available to users.
6. Choose the size of the pool or the number of clones you wish to create on this server.
7. When creating, leave the "sysprep" box checked: this will prepare the reference machine with sysprep, which will then run when the clones are first started.
8. Use the checkbox to either select or deselect the "Linked Clone" option. Using linked clones saves disk space and significantly reduces clone creation time.
9. When configuring the machine, you must enter a number of items of information such as the domain, the domain administrator account and password, and then the local administrator password.

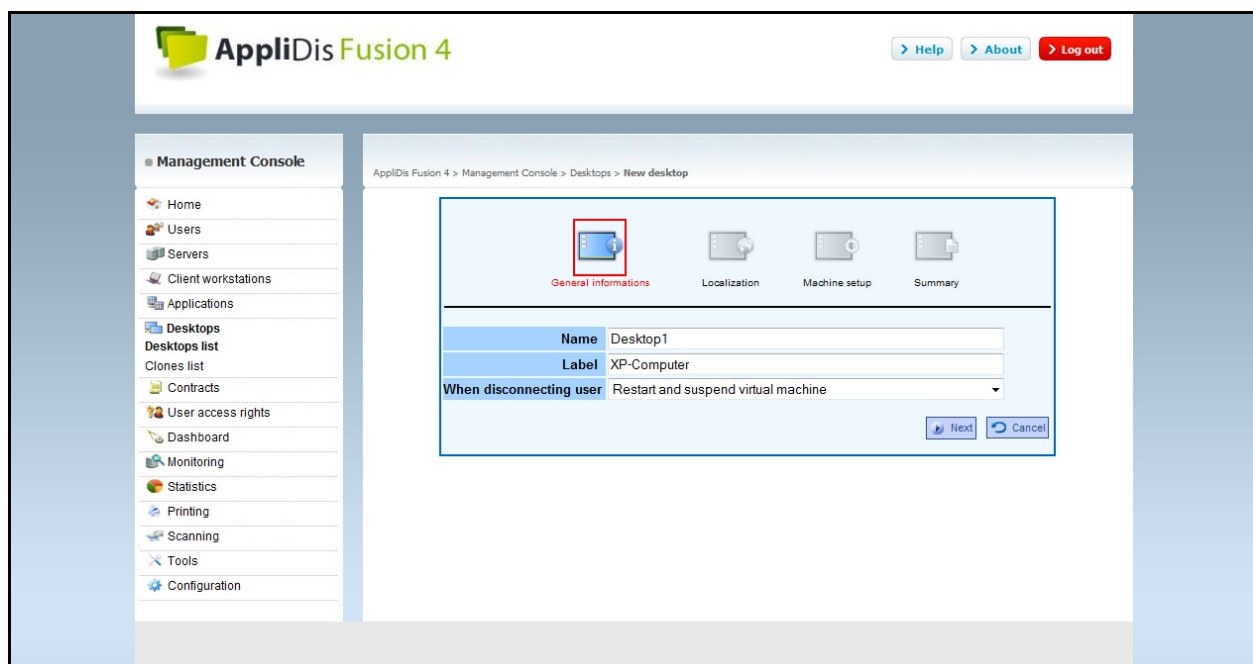


Figure 46 - Desktop creation (step 1)

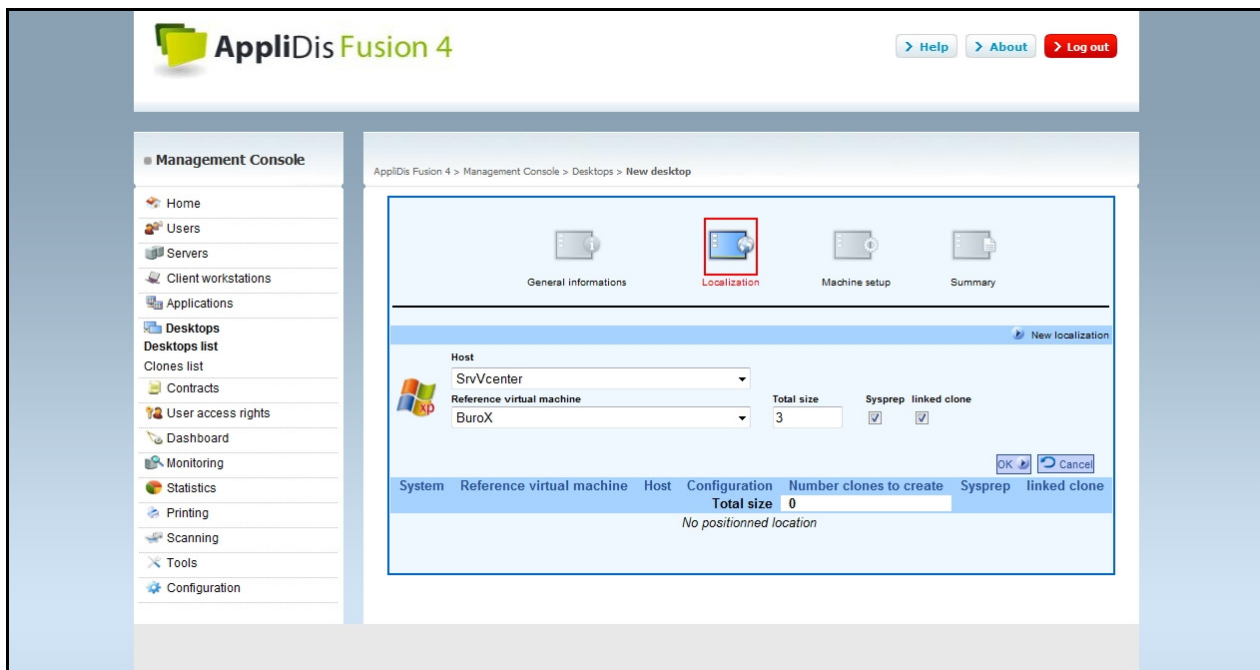


Figure 47 - New desktop creation, localization (step 2)

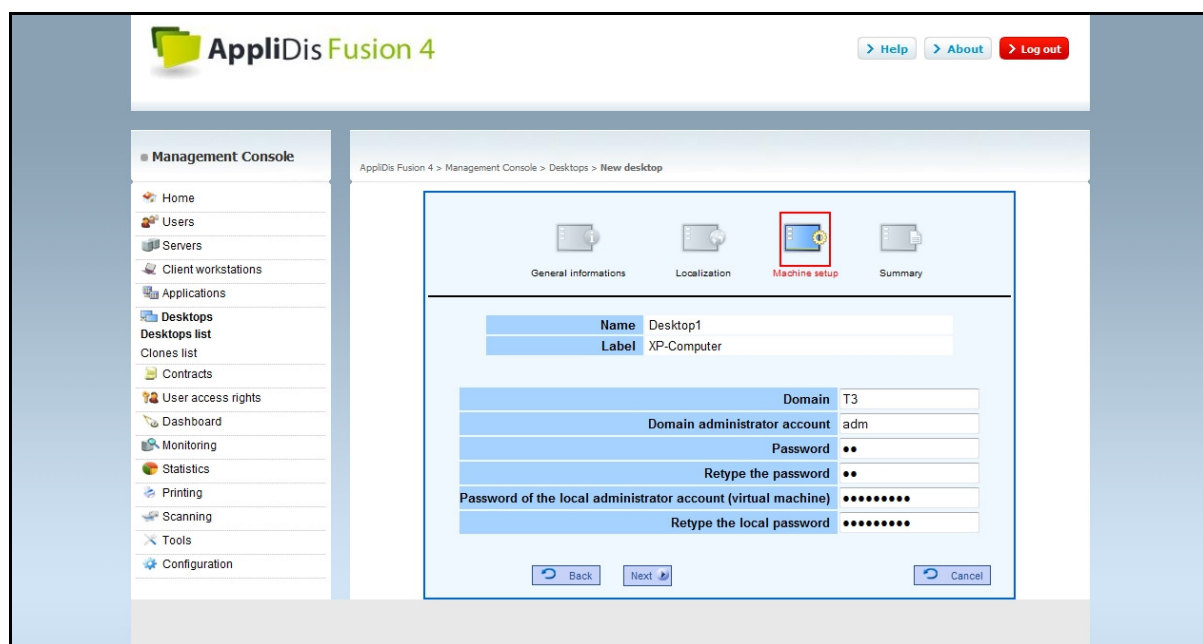


Figure 48 - New desktop creation (Machine setup, step 3)

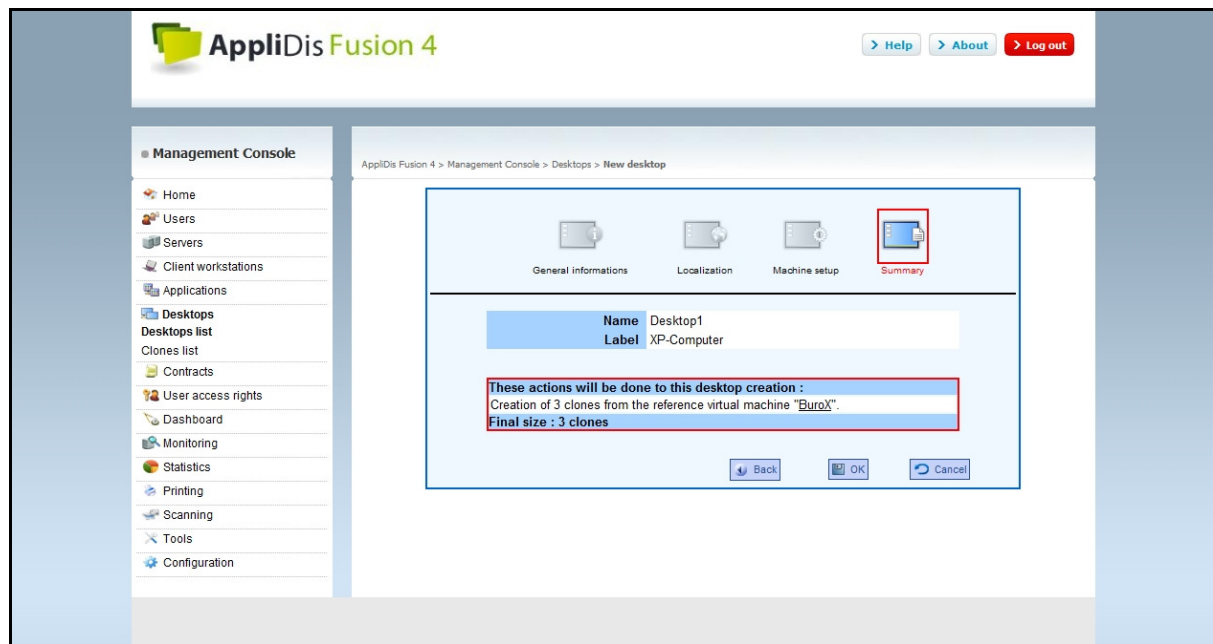


Figure 49 - New desktop creation (Summary, step 4)

Once the desktop has been configured, AppliDis will manipulate the virtual images to make them available to users. The percentage of the work carried out appears in red under the desktop icon, showing you whether the work is complete or not. When this text disappears, all clones are available for use, and you may now create the contract to make them available to users.

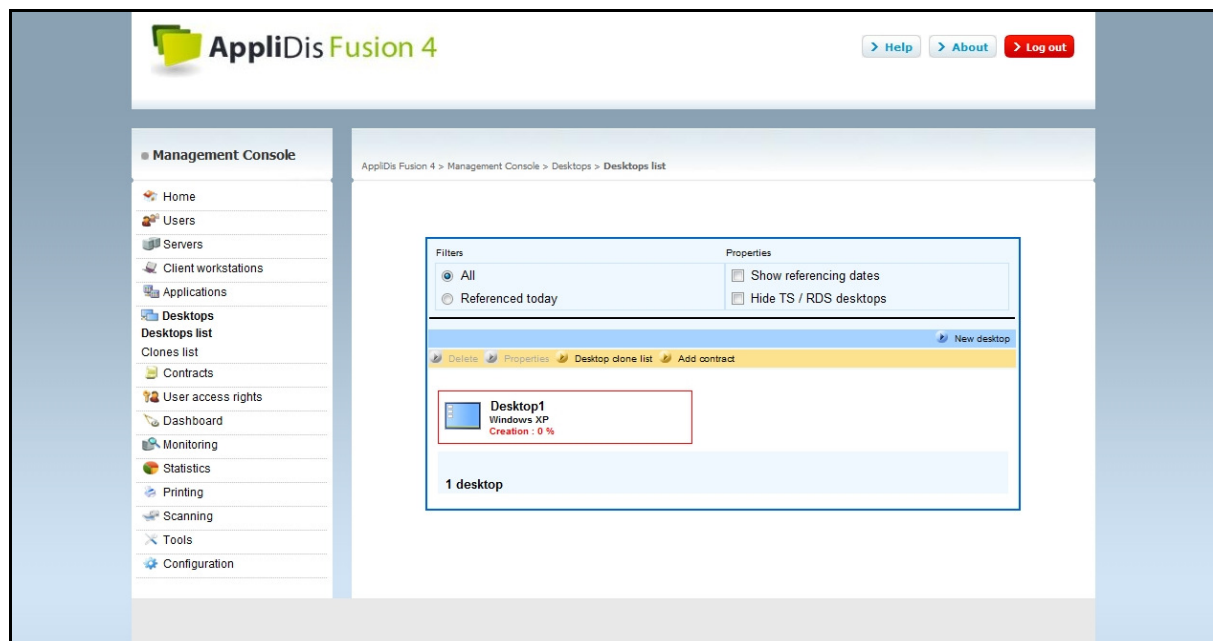


Figure 50 - Desktop creation (percentage %)

Modification of a desktop

You can modify several of the component parts of a desktop. To do this select the desktop then click on Properties.

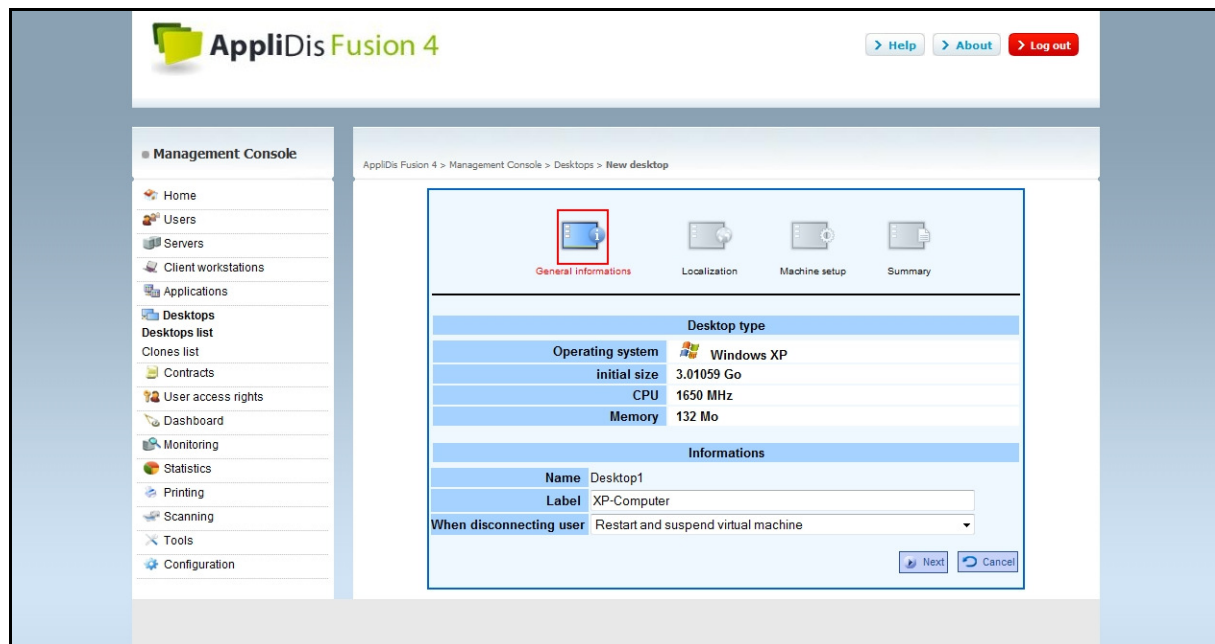


Figure 51 - Desktop properties (General information)

Possible modifications are:

- Description,
- Action to perform upon user disconnection,
- Addition of a new location,
- Modification of an existing location.
- Removal of an existing location

Before adding a new location, you must first have placed the reference image on the new hypervisor.

To modify an existing location, select it from the list of locations and then click the "Edit" button. You may then modify the number of clones. If you set the number of clones to zero, the modification will have the effect of removing locations. If you increase the number of clones, AppliDis Fusion 4 will recreate the new clones on the hypervisor. If the number of clones is reduced, AppliDis Fusion 4 will remove the clones not used by users.

Removal of a desktop

To remove a desktop, select it from the list of desktops and click the "Remove" button. A desktop may only be removed if there is no contract on it.

In addition, the automatically created RDPDesktop cannot be removed.

20.2 List of clones

This list shows all clones created via AppliDis Fusion 4 on the virtual machine host servers.

The display can be simplified by selecting a specific desktop from the pull-down menu.

This list gives a very fast way of checking a machine's status (stopped, paused or running). It also shows the clone's associated desktop, installed system, IP address and status (closed, open). If it

is being used by a user, information about this will appear on the same line (user name, permanent or temporary clone, service status).

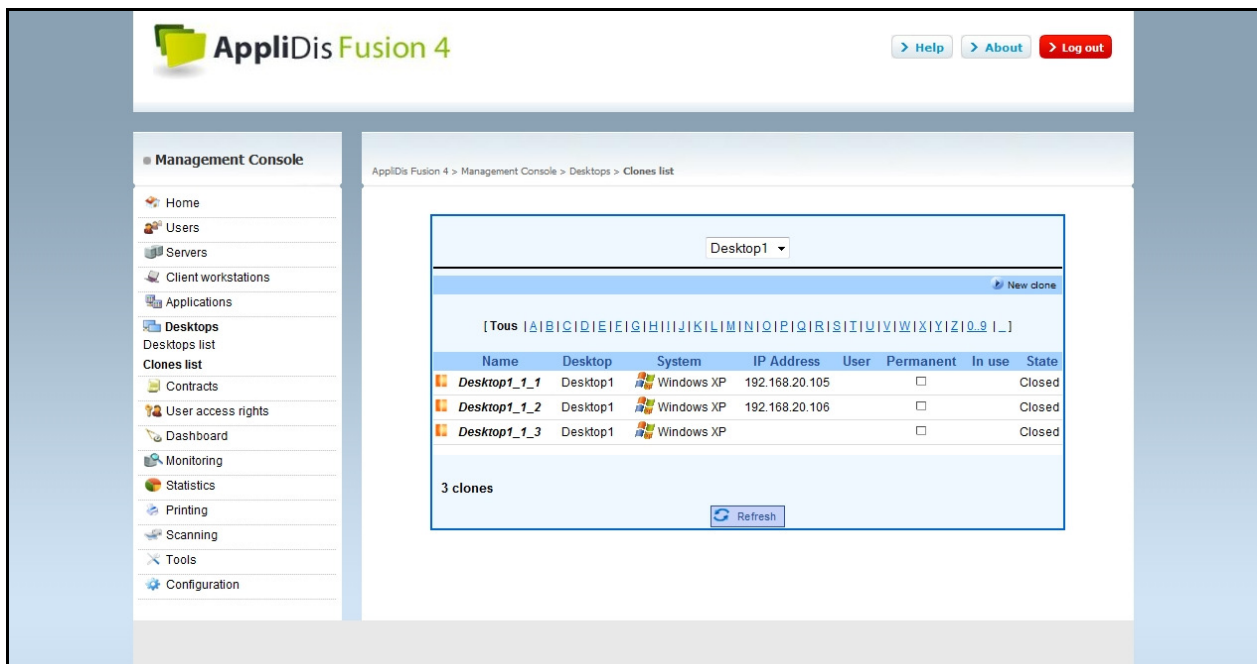
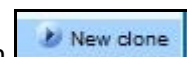


Figure 52 - Clone list

Associating a clone

Associating a clone with a desktop re-establishes the links between a desktop and its clones. There may be a number of possible reasons for the removal of links. The first of these is the disassociation of a clone from a desktop. Another possibility could be the result of a crash on the physical machine and the identical reinstallation of a configuration. This prevents the need to recreate everything directly via the interface.

To associate a clone with a desktop, click the "Associate a clone" button



The information page appears, requiring you to enter certain items of information:

- Virtual machine; choose the clone to be associated from the drop-down list
- Name of the desktop instance; by default, the name will be set to the name of the clone.
- Linked clone; this checkbox allows you to specify whether or not the clone is linked to its initial image.
- Selection of the desktop with which you wish to associate this clone.
- Reference virtual machine; select the reference virtual machine from which the clone was created from the drop-down list. This list is filled with the definition of the desktop, so when you select the desktop, the list will be very short.

The screenshot shows the 'Management Console' interface of AppliDis Fusion 4. The left sidebar contains a navigation menu with options: Home, Users, Servers, Client workstations, Applications, Desktops, Desktops list, Clones list, MyApps Catalog, Contracts, User access rights, Dashboard, Monitoring, Statistics, Printing, Scanning, Tools, and Configuration. The main content area displays the breadcrumb 'AppliDis Fusion 4 > Management Console > Desktops > New clone'. A central form titled 'Informations' is used for creating a new clone. It contains the following fields:

Virtual machine	Seven_1_2
Desktop instance name	Seven_1_2
linked clone	☒
Desktop	Seven
Reference virtual machine	SH-XP_Client

At the bottom of the form are two buttons: 'OK' and 'Back'.

Figure 53 - New clone to be associated

After validation, the clone appears in the list along with all its associated information.

Properties of clones

The "properties of a clone" function enables consultation of all information regarding the selected clone.

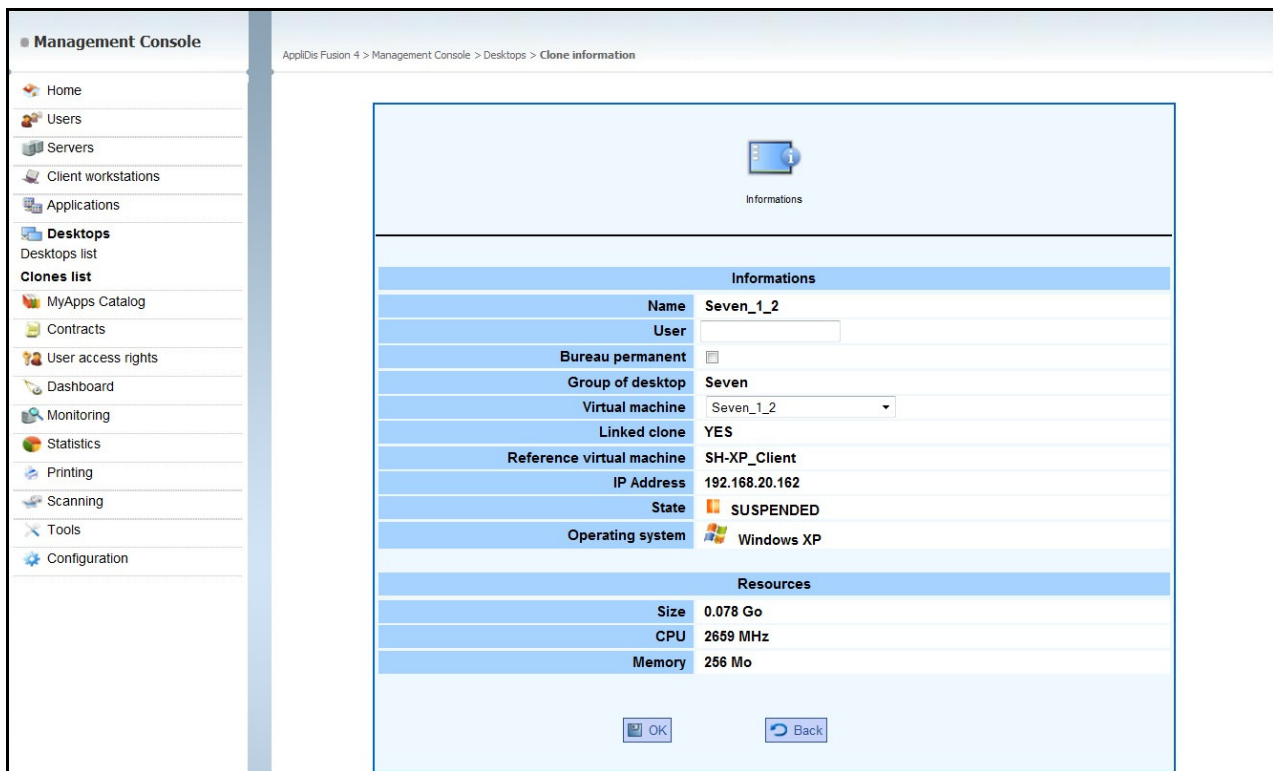


Figure 54 - Clone information & properties

Remove a clone

Removing a clone destroys the selected clone and removes its reference from the pool of desktops. It is possible to remove a clone regardless of its state. If a user is connected to the clone, it will then be automatically reinitialised and the clone will be removed.

Disassociating a clone

Disassociating a clone removes the reference to the clone from the pool of desktops to which it had previously been associated, but in this case it is not destroyed on the hypervisor.

To disassociate a clone, select it from the list and click on the "Disassociate" button.

Maintenance

It is possible to switch a clone to "maintenance" status, which will prevent users from connecting to that clone. This maintenance status can be reversed, making the clone available again to users, at any time.

To set a clone's status to "maintenance", select it in the list then click on the "Maintenance" button. Following a validation request, the clone is then unavailable for users and the clone's line on the list changes to red to indicate "maintenance" status.

To take a clone out of "maintenance" status, select a clone which has a red line, then click on the "Maintenance" button. The clone is then free again for user access and the colour of the clone's line in the list goes back to black.

Greyed-out

It is possible for a clone's line to be greyed out. There are several possible reasons for this: either because the clone cannot be contacted following a network failure, in which case it will cease to be

greyed out once it becomes accessible again by AppliDis Fusion 4, or because the image has been removed; for example, via the hypervisor administration tools or manually at the disk level. In this case, you can either remove or disassociate the clone, and it will no longer appear on the list of clones.

21 Contract Management

21.1 Contract principle

The contract is the element binding a user group to a particular application, application group or desktop, following certain parameters (duration and number of simultaneous users). These contracts give usage privileges to the various users selected through their group.

The contract is defined by:

- An available application in the list of applications, an application group or a desktop. It applies to the application or all the applications contained in the application group or even the desktop to which access is authorized.
- A group of users or an Organizational Unit. The members of this group or Organizational Unit will have the right to execute the defined application.
- A contract start date.
- A contract end date or the selection of an unlimited mode allowing a contract without an end date.
- A number of authorized simultaneous users.

After having created a contract, the users in question are automatically given access to the applications and/or desktops specified in the contract: these applications and/or desktops appear in their applications portal, in AppliDis Desktop and in the virtual desktop. Even if a user holds several contracts for the same application, for example as a result of belonging to several user groups, the application will still only appear once.

Moreover, a contract on an application group gives access to all the applications contained in the group. If this application group receives a new application after the creation of the contract, the user will automatically see this new application. Conversely, if an application is removed from an application group (having a contract), this is automatically removed (unless it is granted by another contract).

All contracts can be seen in the "Contracts" menu. There are three kinds of contracts (contracts on applications, contracts on application groups or contracts on desktops). Contracts on applications are indicated by blue icons, contracts on application groups by yellow icons and contracts on desktops by mauve icons.

If a contract is placed on an application group, the user sees on the application portal the whole application group gathered within a framework bearing the name of this group.

If a contract is placed on an application, the user sees this application displayed on the portal in a frame bearing the name of the application group to which it belongs. If it belongs to several groups, it will be displayed in several frames (one frame per group). Lastly, if it does not belong to any group, it will be displayed in a group called "Default".

21.2 Adding a contract

You can add two different kinds of contracts:

Adding a contract for an application

If no application is available in AppliDis, the "contract type" category described below does not allow the "on an application" option to be selected. Only contracts on application groups are then authorized (provided in the following paragraph).

1. Click on Contracts in the main menu.
2. Click on New contract.
3. In type of contract, select the "On an application" option.
4. Select the desired application from the Applications list.
5. Select the user group authorized to use this application from the Group list.
6. Click on the Contract start date button to indicate the start date for this contract.
7. Click on the Contract end date button to indicate an end of contract or on the Unlimited option if you do not wish to indicate an end date for the contract.
8. Indicate the number of simultaneous users authorized for this contract, in the Maximum simultaneous users box.
9. Click on OK.

Note: The contract start time is automatically 0:00, and its end date is automatically 23:59. If you wish to make an application available for one day only, you must have for example January 2nd, 2005 as the contract start date and January 2nd, 2005 as the contract end date.

It is also possible to add a contract from the Applications heading;

1. Click on Applications in the main menu.
2. Select the desired application.
3. Click on Add contract.

The elements concerning the contract must then be filled in, as previously indicated, and validated to create a new contract.

Adding a contract for an application group

If no application group is available in AppliDis, the "contract type" category described below does not allow the "on an application" option to be selected. If no application is available and if no application group is available, then the "New contract" button does not allow the add contract page to be opened.

1. Click on Contracts in the main menu.
2. Click on New contract.
3. In type of contract, select the on an application group option.
4. Select the desired application group in the List of Application groups.
5. Select the user group authorized to use this application from the Group list.
6. Click on the Contract start date button to indicate the start date for this contract.
7. Click on the Contract end date button to indicate an end of contract or on the Unlimited option if you do not wish to indicate an end date for the contract.
8. Indicate the number of simultaneous users authorized for this contract, in the Maximum simultaneous users box.
9. Click on OK.

Adding a contract for a desktop

If no desktop is available in AppliDis Fusion 4, the "contract type" category described below does not allow the "on a desktop" option to be selected.

1. Click on Contracts in the main menu.
2. Click on New contract.
3. In type of contract, select the on a desktop option.
4. Select the desired application group in the Desktops list.
5. Select the user group authorized to use this desktop from the Group list.
6. Click on the Contract start date button to indicate the start date for this contract.
7. Click on the Contract end date button to indicate an end of contract or on the Unlimited option if you do not wish to indicate an end date for the contract.
8. Indicate the number of simultaneous users authorized for this contract, in the Maximum simultaneous users box. **Warning: this figure may not exceed the number of available clones.**
9. Click on OK.

21.3 Removing a contract

Expired contracts are not deleted, so that their statistics can still be accessed. On the other hand, a contract can be directly removed.

Removing a contract

1. Click on Contracts in the main menu.
2. Select the Contract to be removed from the list by clicking on it.
3. Click on Remove.

21.4 Modifying a contract

The properties of a contract can be modified at any time. It is thereafter possible to change the maximum number of users, the end date or the user group concerned. On the other hand, the application, application group or desktop attribute can no longer be modified.

Modifying contract parameters

1. Click on Contracts in the main menu.
2. Select the Contract to be modified from the list by clicking on it.
3. Click on the Properties button.
4. A page describing the contract will be displayed.
5. Edit the parameters that you wish to change.
6. Click on OK to save the modifications.

22 Management of Privileges

The 'Privileges Management' menu allows the management and viewing of users' server privileges for accessing local disks and printers and permanent desktops.

It thus gives administrators an overall view of the options accessible by the user.

Creation/modification/removal of user privileges for accessing local disks and printers and permanent desktops is managed from the Users menu. Refer to part "

User management" p. 66.

22.1 Management of server privileges

Access privileges on servers

By default, privileges are set to enable access by user groups to all servers. There is no need to modify them unless you wish to prohibit access to one or more servers for a collection of users.

1. Click on Access privileges in the main menu.
2. Select User group privileges/server from the horizontal menu.
3. Select the entity for which you wish to search the server privileges from the Groups or Organizational Units list on the right.
4. Select the server which you wish to remove from the same list, then click on Remove. A server is added by selecting it from the Server group, then clicking on the right arrow.
5. Click on OK.

22.2 Management of application privileges

Checking the application privileges for a user

Privileges are checked under the Access privileges section. This tool allows the AppliDis administrator to display the portal of an AppliDis user.

Note: This menu is only available in **synchronized** mode. In dynamic mode, you can view a user's portal by means of the **Search** menu (see page 78, Searching for a user)

1. Click on Access privileges in the main menu.
2. Click on the User privileges / application sub-menu.
3. From the Users list, which shows the users having access to AppliDis, select the user for which you wish to search the privileges by applications.

You can also access the privileges page from the user menu:

1. Click on Users in the main menu
2. From the list of users, select the desired user by clicking on his user name.
3. Click on Privileges, then select the Users/application privileges tab.

22.3 Management of option privileges

Checking the option privileges for a user group

The privileges are checked under the **Access privileges** section.

1. Click on Access privileges in the main menu.
2. Select User groups privileges/Options from the horizontal menu.
3. Select from the Options selection box the option for which you wish to display the authorized groups (Access to disks, Access to local printers or permanent desktops).
4. In the list on the right, Options for Groups/OUs, you can see the groups/OUs authorized for the selected option.
5. You can select the groups/OUs that you wish to remove from the same list.
6. In the list on the left, Groups/OU present in AppliDis, you can select groups/OUs and add them to the list on the right by clicking on the right arrow to give them access to the selected option.
7. Click on OK.

23 Using the dashboard

23.1 Principle of the Dashboard

The AppliDis Dashboard makes it possible to follow AppliDis activity on your various Application host servers, virtual desktops and virtual machine host servers in real time. It is thus possible to know the number of connected users and the desktops and applications in use, and to execute various actions, such as deactivating an Application Server. Actions such as remote takeover or the sending of a message to a user while an application is being executed are also possible.

23.2 Viewing the information

Viewing instantaneous information for servers

To access this information:

1. Click on Dashboard in the main menu.

The page is displayed and shows the following information for each available server:

- % CPU: the last instantaneous CPU usage collected for this server.
- Users: the number of users currently using AppliDis.
- Applications: the number of applications currently in use.

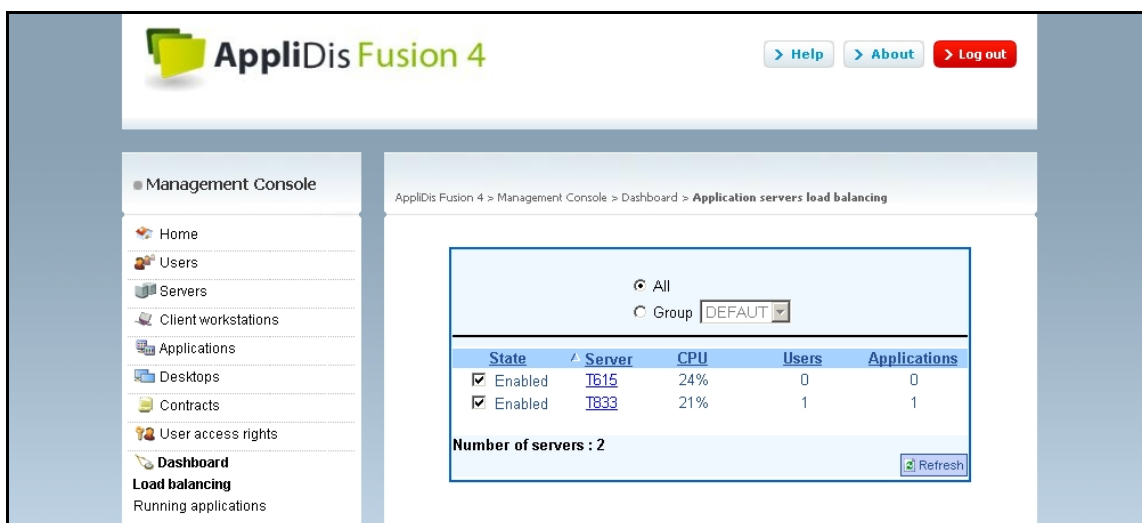


Figure 55 - Example of general view of the Dashboard (application servers load balancing)

Viewing the applications in use

To obtain a detailed list of the applications in use:

1. Click on **Dashboard** in the main menu.
2. Click on **Applications in progress**.

In the "**Applications in progress**" menu, servers, applications or users can be filtered via a selection list and a data entry field. Click on the Search button to display the result.

The list of applications in progress can be sorted in ascending or descending order by user, application or server by clicking on the heading of the corresponding column.

Two new options have been added:

1. to send message to all the users sorted via the filter.
2. to reset all the sessions sorted via the filter.

These two new options apply to all the users selected via the filter.

Warning: if you did not select a filter, clicking on the **"reset"** button will reset all the users currently connected to the AppliDis server farm. A confirmation message will then enable you to validate your choice to reset all applications.

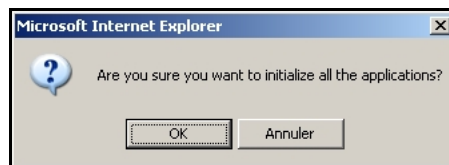


Figure 56 - Confirmation box

The information on the page will be refreshed by clicking on the **"Update"** button which is located below and to the right of the list, or automatically.

The total number of connected users of the **"Connected users"** sub-menu which were removed, will now be in the **"Applications in progress"** sub-menu in the form:

"Total of 100 applications for 68 connected users".

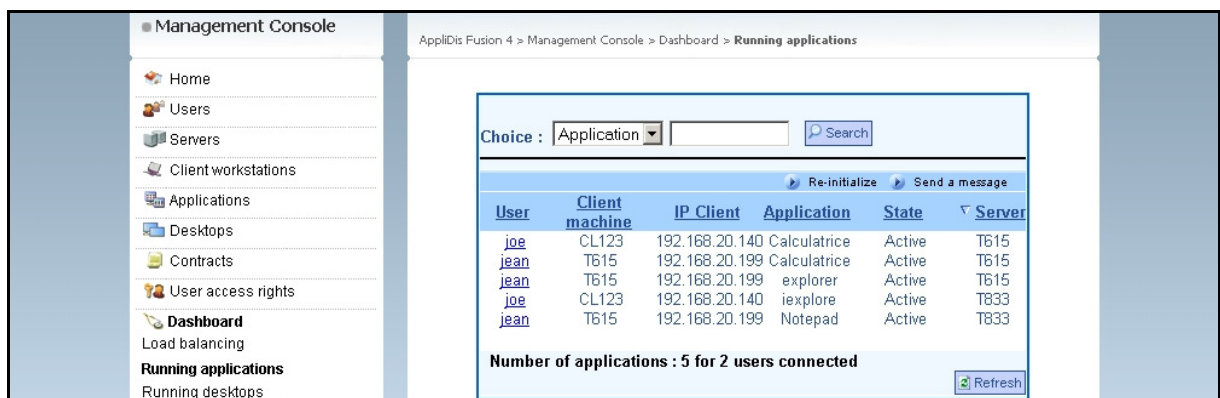


Figure 57 - Dashboard - applications in progress

Viewing the applications in use

To obtain a detailed list of desktops currently in use:

1. Click on **Dashboard** in the main menu.
2. Click on **Desktops in progress**

In the **"Desktops in progress"** menu, users or desktops can be filtered via a selection list and a data entry field. Click on the Search button to display the result.

The list of applications in progress can be sorted in ascending or descending order by user, client workstation, IP client, desktop, Status, Virtual Machine or Connection Date by clicking on the heading of the corresponding column.

Two new options have been added:

1. Option to send message to all the users sorted via the filter.
2. Option to reset all the sessions sorted via the filter.
3. Option to disconnect all the sessions sorted via the filter.

These new options apply to all the users selected via the filter.

Caution: if you did not select a filter, clicking on the **"reset"** button will reset all the users currently connected to the AppliDis server farm. A confirmation message will then enable you to validate your choice to reset all desktops.

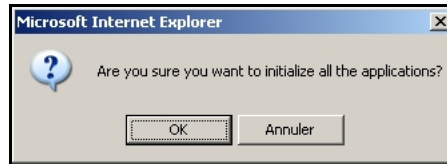


Figure 58 - Confirmation box

The information on the page will be refreshed by clicking on the **"Update"** button which is located below and to the right of the list, or automatically.

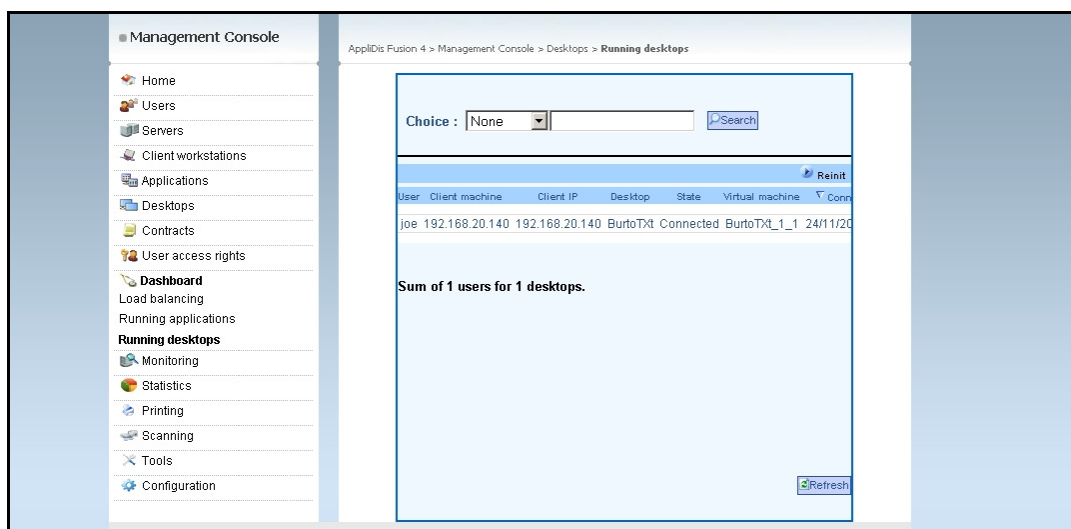


Figure 59 - Dashboard (running desktops in progress)

23.3 Deactivate a server

In certain cases, it may be necessary to temporarily stop the use of an AppliDis application and Windows desktop host server. For example, in order to prevent users connecting to this server if maintenance operations are required on the server. Deactivating a server **does not cause** the disconnection of the users working on this server by AppliDis. A server can only be deactivated or activated by the group of administrators from the Active Directory domain.

Note: An Application and Windows desktop host Server can also be deactivated directly from Windows by stopping the "AppliDis Application server" service.

Deactivating a server

1. Click on **Dashboard** in the main menu.
2. Uncheck the **Activated** box on the line of the server to be deactivated,.

The box will be unchecked and the word Activated shown in red; the counters will no longer be updated more.

Note: Warning: after rebooting a deactivated server, it will be automatically re-incorporated into the server

farm as an active server.

Activating a server

1. Click on **Dashboard** in the main menu.
2. Check the **Activated** box on the line of the server to be activated.

If activated, when the server is activated the check box will become shaded during startup. Once activation has finished, the box will be checked and the word Activated will be shown in black. The counters will be updated once more.

23.4 Interacting with current applications

Applications which are current but disconnected appear in greyed-out form.

When an application is selected, it is surrounded by a red box. If several applications are surrounded by red, this means that they are being executed in the same session. Consequently, all the actions relating to one application (sending of messages, disconnection, takeover, rebooting) will also relate to the others.

Different possible actions:

Taking control of an application

The administrator can take control of an application currently being run by a user. This enables the administrator to provide support for a usage problem or to deliver training:

1. Click on **Dashboard** in the main menu.
2. Click on **Applications**.
3. Select the application for which you wish to take control, then click on **Take control**.

Upon taking control, the user in question will see a request to accept or refuse the takeover. If the user accepts, the administrator will have control over his application (This behavior depends on the system parameter settings).

The default behaviour is as follows: the user and the administrator can use the keyboard and mouse to interact with the application.

Rebooting

Rebooting an application definitively stops the application with no possibility of going back. The user can no longer cancel the administrator's action.

1. Click on **Dashboard** in the main menu.
2. Click on **Applications in progress**.
3. Select the application to be rebooted, then click on **Reboot**.
4. A request for confirmation will be displayed and must be validated to definitively reboot the application.

Sending a message

The administrator can send a message to a user running a particular program. The message will appear only to the user in question, in the form of a dialog box.

1. Click on **Dashboard** in the main menu.
2. Click on **Applications in progress**.
3. Select the application for which you wish to send a message, then click on **Send a message**.
4. Enter a Title and a Message then click on OK to send the message.

Disconnecting

The administrator can disconnect an application. In this case, the application will continue to be executed on the server, but the user will lose his session in progress. The session will then be available for the user in his "Disconnected applications" page on the portal.

1. Click on **Dashboard** in the main menu.
2. Click on **Applications in progress**.
3. Select the application to be disconnected, then click on **Disconnect**.
4. A request for confirmation will be displayed and must be validated to disconnect the application.

Note: The aforesaid operations may require the addition of certain "Terminal Server" parameter settings on the AppliDis Application Servers. Takeover, for example, requires the setting of the takeover privilege in the TSE services configuration.

23.5 Interacting with current desktops

Desktops which are current but disconnected appear in greyed-out form: the disconnection date/time is shown below the desktop icon.

When a desktop is selected, it is surrounded by a red box.

Different possible actions:

Rebooting

Rebooting a desktop definitively stops the desktop with no possibility of going back. The user can no longer cancel the administrator's action.

1. Click on **Dashboard** in the main menu.
2. Click on **Desktops in progress**.
3. Select the desktop to be rebooted, then click on **Reboot**.
4. A request for confirmation will be displayed and must be validated to definitively reboot the desktop.

Sending a message

The administrator can send a message to a user running a particular desktop. The message will appear only to the user in question, in the form of a dialog box.

1. Click on **Dashboard** in the main menu.
2. Click on **Desktops in progress**.
3. Select the desktop for which you wish to send a message, then click on **Send a message**.
4. Enter a Title and a Message then click on OK to send the message.

Disconnecting

The administrator can disconnect a desktop. In this case, the desktop will continue to be executed on the server, but the user will lose his session in progress. This session will subsequently be available to users on their "**Your desktops**" portal page. The desktop will be greyed out and the disconnection date/time will be shown under the desktop in question.

5. Click on **Dashboard** in the main menu.
6. Click on **Desktops in progress**.
7. Select the desktop to be disconnected, then click on **Disconnect**.
8. A request for confirmation will be displayed and must be validated to disconnect the desktop.

24 Alarm monitoring and reporting

The "Monitoring" menu of the AppliDis administration console can be used to view the feedback of logs from all your AppliDis servers.

The following information is available:

- Application, Security and System Event logs.
- System resources with information on disk resources, RAM resources, CPU resources, etc.
- Terminal Server resources with information such as number of open sessions, disconnected sessions, out of service sessions, etc.
- Alarms set by the administrator on various criteria.
- A module for sending e-mails which makes it possible to define the recipients of the e-mails.

24.1 Viewing the event logs

1. Click on **Monitoring** in the main menu.
2. Go to the **Events** sub-menu.
3. Click on one of the event type buttons: Application, Security or System.
4. You can filter the alarms displayed by Server group, Server role.(administration, application, Gateway), Message type (Error, warning, Information for Application and System logs, Failure audits and Security success audits).
5. Select the day for which you wish to display the messages by clicking on the Date button.
6. Click on Search.
7. The search result will then be displayed.

The figures below show two examples of searches for events of the **Security** and **System** type. The data can also be sorted by clicking on the headings of the table once the search results have been displayed. For reasons of security, the period that can be viewed is limited to one day. The date must be specified when the search is started, as indicated below.

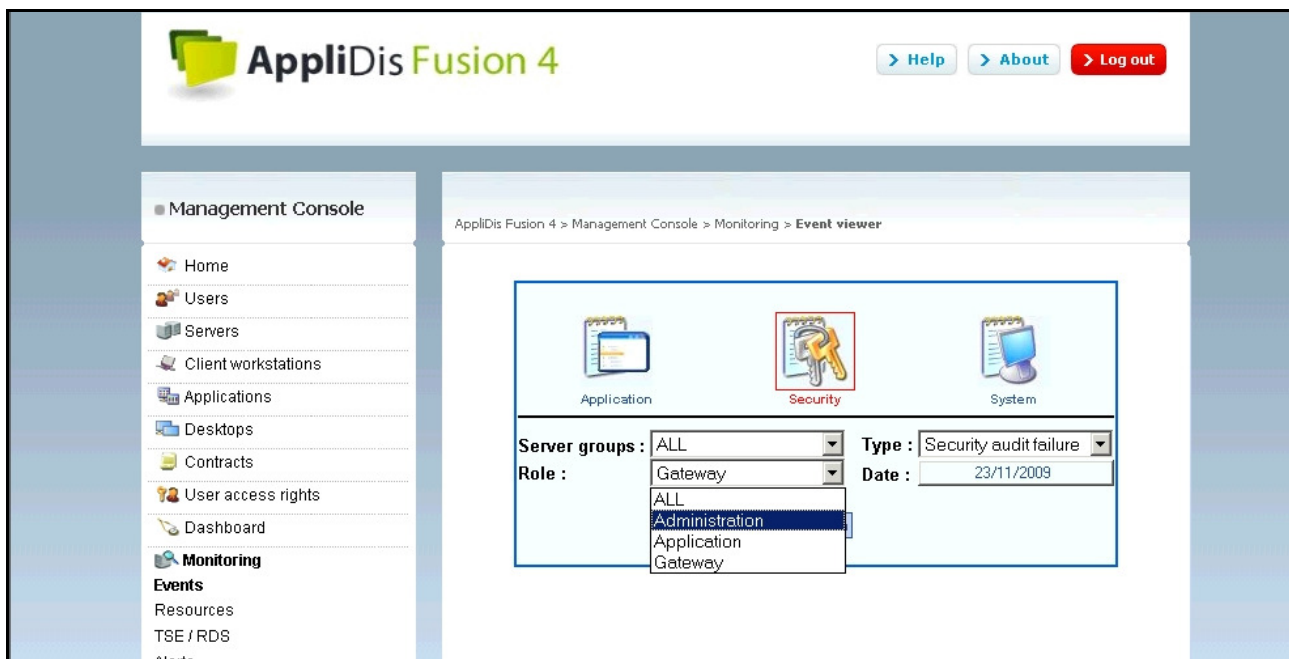


Figure 60 - Search for security events on AppliDis servers

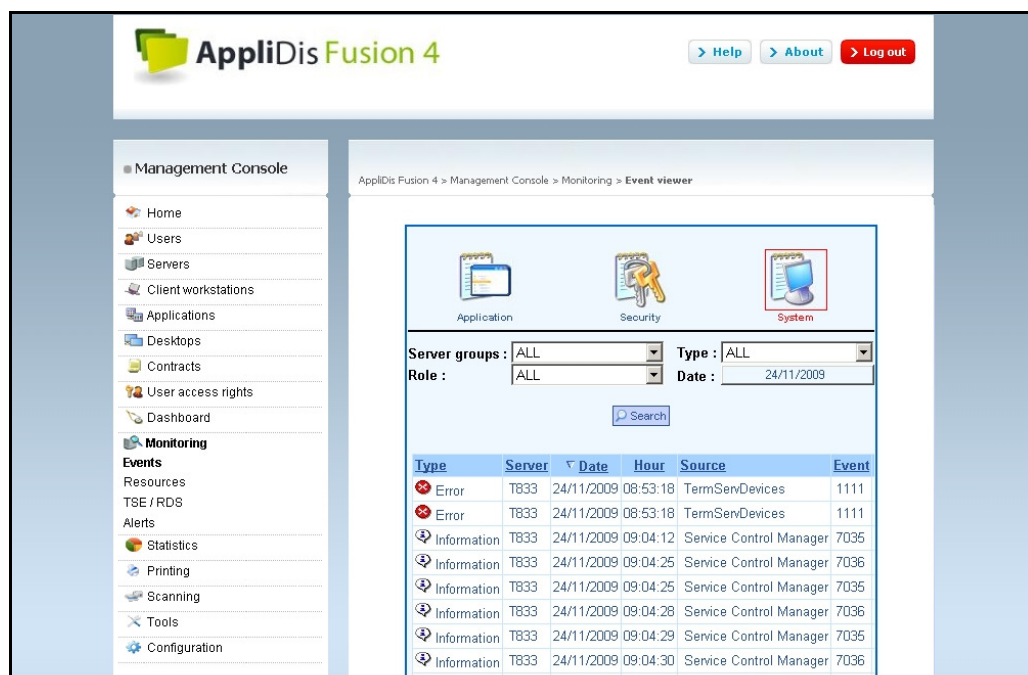


Figure 61 - Display of system information for all servers

For feedback regarding server resources, the administrator can also use filters on the server groups or the server roles (Application servers, Gateway or administrators).

The display of information on Microsoft TSE sessions can also be filtered by server groups.

24.2 Viewing the resources

Viewing resources of the servers allows you to quickly see what are the most used resources on your server farm.

Indeed you can review the amount of used space vs the amount of available disk space.

In the same idea you can view the amount of memory used vs the amount of space available memory space.

But also the amount of CPU consumed.

All this information is instant data and offer an infrastructure view at T time. This enabling you to predict the rise your platform or verify that your platform is properly sized.

1. Click on Monitoring in the main menu.
2. Go to the Resource sub-menu.
3. Click on one of the buttons to display resources of the following types: Disks, RAM or CPU.
4. You can filter the displayed information by Server group or Server role (administration, application, Gateway).
5. Click on Search.
6. The search result will then be displayed.

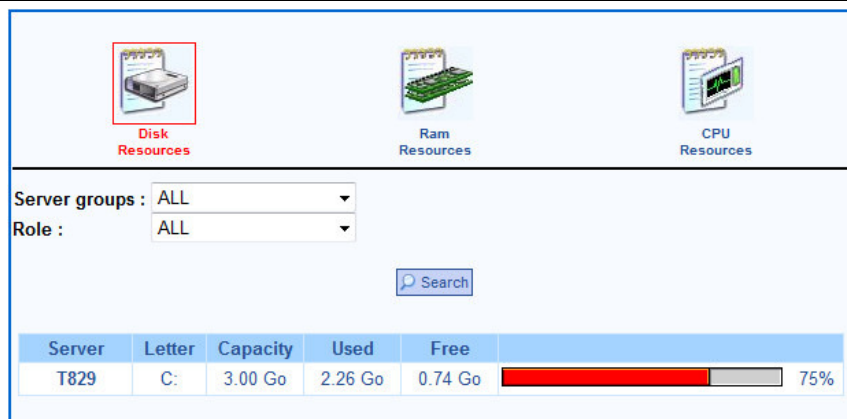


Figure 62 - Viewing disks resources

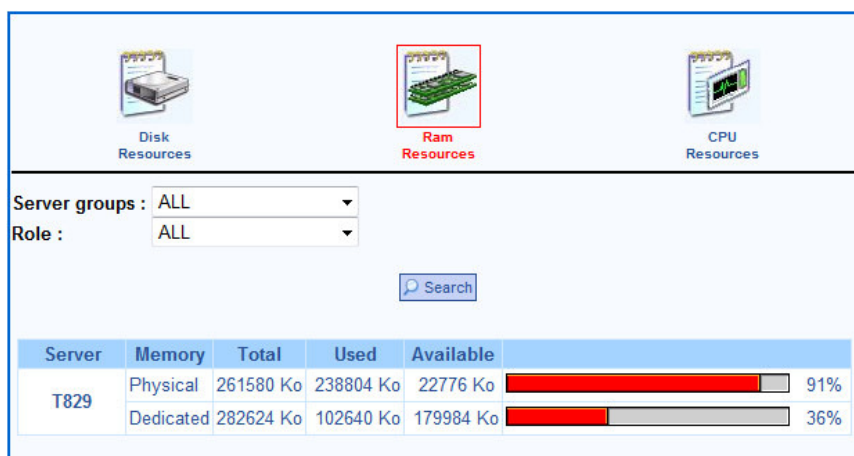


Figure 63 - Viewing memory resources

PHYSICAL = this is the physical RAM (Random Access Memory), as the drawing shows we are talking about the 'memory module' within the machine.

DEDICATED = 'Paging, Swap', which is an important part of virtual memory implementation in most contemporary general-purpose operating systems, allowing them to use disk storage for data that does not fit into physical RAM.

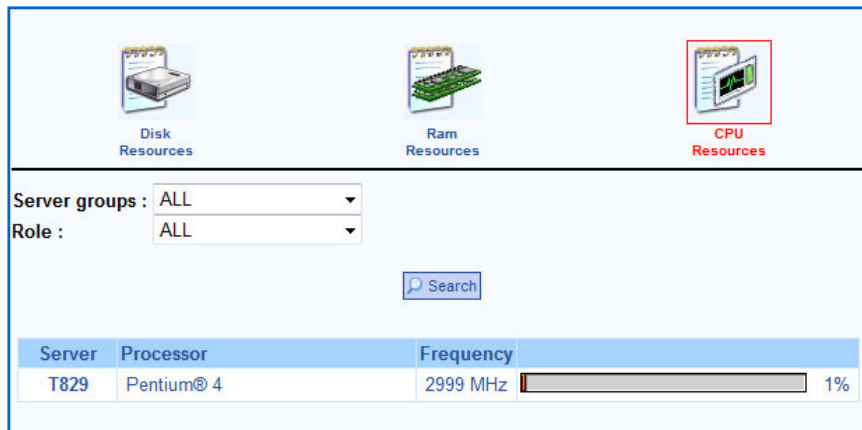


Figure 64 - Viewing CPU resources

24.3 Viewing Microsoft TSE sessions

1. Click on Monitoring in the main menu.
2. Go to the TSE sub-menu.
3. You can filter the displayed information by Server group.
4. Click on Search.
5. The search result will then be displayed.

24.4 Alarm settings

It is possible to activate alarm reports by e-mail or SNMP via the AppliDis administration console. To activate the monitoring module:

1. Click on Monitoring in the main menu.
2. Go to the Alarms sub-menu.
3. Check the Activation of standard alarms on each server checkbox.
4. You can activate and set various Alarms.
5. Click on OK at the bottom of the page. (Next for the initial configuration)

When the **Activation of standard alarms on each server** box is checked, you can activate or deactivate each individual Alarm. Depending on the type of alarm, you can set the **trigger condition**. (Exceeding a threshold value in number, percentage or number per day). For all available alarms, a **monitoring frequency** field (in seconds) enables you to set the frequency with which the monitored element is checked. The **default value** button sets the default values for all monitored elements.

The alarm thresholds for the following criteria can be set from the administration console (see figure below):

- Non-availability of an AppliDis server.
- Non-availability of the AppliDis database.
- Microsoft TSE/RDS session (Out of service).
- Total physical memory exceeded.
- Processor use overload.
- Free disk space.
- Application events observer (Error or Error/Warning).
- Security events observer (Failure audit).
- System events observer (Error or Error/Warning).
- Size of processor queue.
- Remaining AppliDis licenses.
- Handles exceeded (AppliDis Application Server).
- Physical memory MB exceeded (AppliDis Application Server).
- Processor use exceeded (AppliDis Application Server).
- Service unavailability (AppliDis Application Server).
- Handles exceeded (AppliDis Monitor Server).
- Physical memory MB exceeded (AppliDis Monitor Server).
- Processor use exceeded (AppliDis Monitor Server).
- Service unavailability (AppliDis Monitor Server).
- Handles exceeded (AppliDis Redundancy Server).
- Physical memory MB exceeded (AppliDis Redundancy Server).
- Processor use exceeded (AppliDis Redundancy Server).
- Service unavailability (AppliDis Redundancy Server).
- Handles exceeded (AppliDis Gateway Server).
- Physical memory MB exceeded (AppliDis Gateway Server).
- Processor use exceeded (AppliDis Gateway Server).
- Service unavailability (AppliDis Gateway Server).
- Handles exceeded (Microsoft Internet Information Server service).
- Physical memory MB exceeded (Microsoft Internet Information Server service).
- Processor use exceeded (Microsoft Internet Information Server service).
- Service unavailability (Microsoft Internet Information Server service).
- Recycling of IIS pool (Microsoft Internet Information Server service).

AppliDis Fusion 4 > Management Console > Monitoring > Alerts

Standard warnings Monitoring authority Alert diffusion settings

☒ Activate standard warnings on each server

Enabled	Monitored item	Trigger	Control periodicity	Delay
General infrastructure				
☒	AppliDis Server unavailable	Server unavailable	60 s	
☒	AppliDis Database unavailable	Database unavailable	30 s	
☒	TSE / RDS Session (Down)	Nbr ≥ 4	600 s	
☒	Total physical memory overflow	% ≥ 90	300 s	1500 s
☒	Processor overstepping	% ≥ 100	30 s	600 s
☒	Free disk space	% ≤ 20	600 s	
☒	Application events viewer	Error Nbr/day ≥ 1	600 s	
☒	Security events viewer (Security audit failure)	Nbr/day ≥ 1	600 s	
☒	System events viewer	Error Nbr/day ≥ 1	600 s	
☒	Processor queue length	Nbr ≥ 10	60 s	
☒	AppliDis licences	Nbr ≤ 5	60 s	
AppliDis Application Server				
☒	Handles	Nbr ≥ 500	60 s	
☒	Physical memory (Mo)	Nbr ≥ 100000	60 s	
☒	Processor overstepping	% ≥ 90	60 s	
☒	Service unavailable		60 s	
AppliDis Monitor Server				
☒	Handles	Nbr ≥ 500	60 s	
☒	Physical memory (Mo)	Nbr ≥ 100000	60 s	
☒	Processor overstepping	% ≥ 90	60 s	
☒	Service unavailable		60 s	
AppliDis Redondeur Server				
☒	Handles	Nbr ≥ 500	60 s	
☒	Physical memory (Mo)	Nbr ≥ 100000	60 s	
☒	Processor overstepping	% ≥ 90	60 s	
☒	Service unavailable		60 s	
AppliDis Gateway Server				
☒	Handles	Nbr ≥ 500	60 s	
☒	Physical memory (Mo)	Nbr ≥ 100000	60 s	
☒	Processor overstepping	% ≥ 90	60 s	
☒	Service unavailable		60 s	
Internet Information Services				
☒	Handles	Nbr ≥ 500	60 s	
☒	Physical memory (Mo)	Nbr ≥ 100000	60 s	
☒	Processor overstepping	% ≥ 90	60 s	
☒	Service unavailable		60 s	
☒	IIS Recycling pool		60 s	

Default values Next Cancel

Figure 65 - End of alarm parameter setting

24.5 Definition of the Monitoring authority

The monitoring authority is a specific account user having Local Administrator privileges on all the servers to be monitored, therefore, all the servers in the AppliDis farm: Administration and Connection Broker servers, Web User Portal servers, Gateway servers and application and Windows desktop host servers. This account is used by the service to remotely question the various servers using the Microsoft WMI interface. It is essential for the operation of the monitoring module.

1. In the Monitoring/Alarm menu, click on Monitoring authority (for the initial configuration, clicking on Next at the previous step leads to this page).

2. Fill in the Domain name.
3. Fill in the Account used.
4. Fill in the password and confirmation.
5. Click on OK (Next for the initial configuration).

Note: The account set up for the monitoring authority must have Local Administrator privileges on **all** AppliDis servers for access to information feedback returned via WMI.

Figure 66 - Monitoring authority parameter setting

24.6 Definition of information transmission methods

The administrator can arrange for information to be sent by e-mail when an alarm is triggered. Follow the procedure below to parameterize the reception of alarm e-mails:

1. In the Monitoring/Alarm menu, click on People to inform (for the initial configuration, clicking on Next at the previous step leads to this page).
2. Fill in the SMTP server.
3. Fill in the Sender.
4. To add recipients, enter an e-mail address in the Add recipient field, then click on the down arrow.
5. Click on OK.

Note: This function of sending alarms requires the presence of an SMTP service set to accept the sending of e-mail from the AppliDis administration server hosting the service.

The sending of alarm e-mails for a type of alarm for a given server is limited to 25 e-mails sent per day. The last message sent specifies to the recipients that the limit has been reached.

The screenshot displays the 'Alert diffusion settings' configuration window. At the top, there are three tabs: 'Standard warnings', 'Monitoring authority', and 'Alert diffusion settings' (which is selected). Below the tabs, there are two main sections:

- Enable SNMP alerts:** This section includes fields for 'SNMP Manager IP' (127.0.0.1), 'Port' (162), 'Community' (public), and 'OID Prefix' (.1.3.6.1.4.1.31368.1). There is a checkbox for 'Enable AppliDis SNMP agent' and two buttons: 'SCOM Export' and 'MIB Export'.
- Enable e-mail alerts:** This section is checked and includes fields for 'SMTP Server' (mail.systancia.com), 'Sender' (S360@systancia.com), and a 'Recipient to be added' field. Below these is a list of 'Recipient(s)' with 'admin01@systancia.com' and 'admin02@systancia.com' listed. There are 'Remove' and 'Remove all' buttons at the bottom of the list.

At the bottom of the window, there are 'Back', 'OK', and 'Cancel' buttons.

Figure 67 - Configuration of alarm recipients

Configuration of alarms by SNMP

AppliDis alarms have been enhanced by being able to send alarms using SNMP protocol besides the existing procedure for sending e-mails.

The configuration for sending SNMP messages has just been added to the existing configuration for sending e-mails in the AppliDis administration console.

Essential requirement: the implementation of SNMP protocol requires installation of the "Microsoft SNMP Agent" service (see page 8 of this document).

Overview of SNMP - Simple Network Management Protocol

SNMP is a **communications protocol** which enables network users to manage network equipment and supervise and diagnose network and hardware problems remotely.

The network management architecture proposed by SNMP protocol is based on two main elements:

- Managed devices are network elements (bridges, switches, hubs, routers or servers), containing "managed objects" contained in a tree-structured database called MIB. These objects can be hardware information, configuration elements or statistical data.
- Agents, i.e. a network management application residing in a peripheral and responsible for transmitting local management data from the peripheral to the network management system in SNMP format.

SNMP protocol also defines a concept of traps. Once this is defined, the agent sends an alarm to the SNMP administration Server if a certain event, such as exceeding a threshold, occurs.

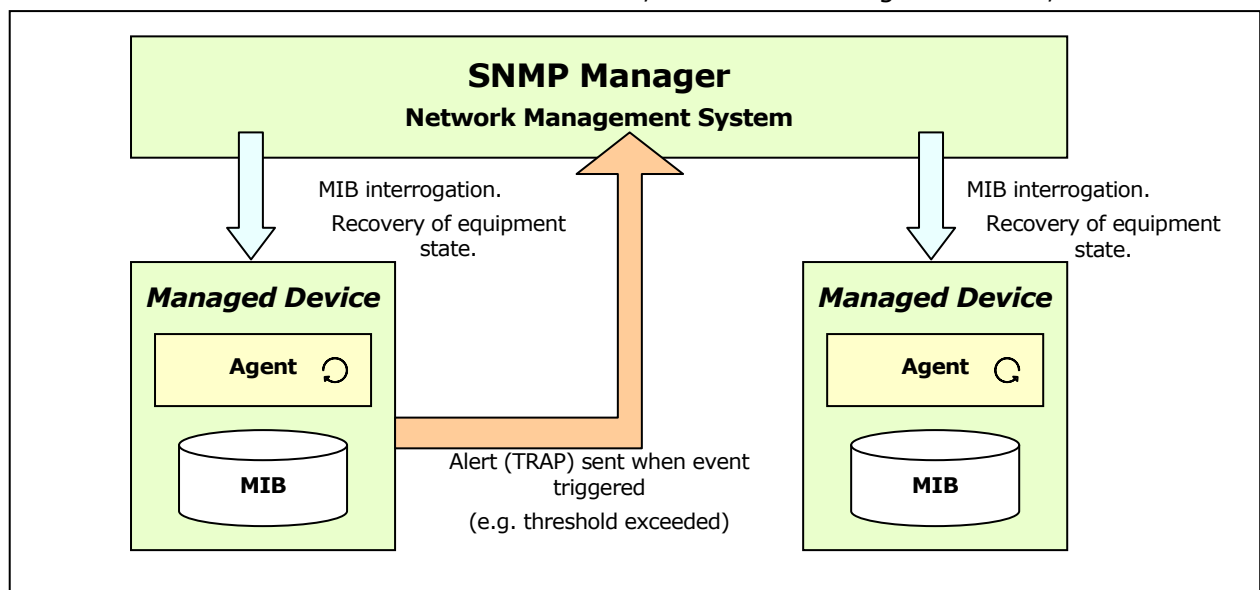


Figure 68 - Descriptive diagram of SNMP protocol

List of AppliDis alarms returned via SNMP

The AppliDis monitoring module (AppliDis Monitoring) reports alarms via SNMP protocol. These trap messages consist of an object identifier (OID) and a descriptive parameter (as a character string) describing the alarm sent. The OID syntax is standardized and consists of a sequence of numbers separated by periods. Each AppliDis OID starts with the number sequence **.1.3.6.1.4.1.31368.1** corresponding to the **.iso.org.dod.internet.private.enterprises.systancia.applidis** identifier.

The list of alarms is shown in the table below.

Information	Alarm trigger	OID of the TRAP
Database		
Database	Database not available	.1.3.6.1.4.1.31368.1.105 .iso.org.dod.internet.private.enterprises.systancia.applidis.databaseAppliDisTrap
Database	Database available again	.1.3.6.1.4.1.31368.1.205 .iso.org.dod.internet.private.enterprises.systancia.applidis .database.databaseAppliDisEndTrap
Equipment		
Memory overflow (RAM)	RAM value exceeded	.1.3.6.1.4.1.31368.1.107 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramAppliDisTrap
Memory overflow (RAM)	RAM value back below threshold	.1.3.6.1.4.1.31368.1.207 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramAppliDisEndTrap
Processor performance overflow (CPU)	CPU value exceeded	.1.3.6.1.4.1.31368.1.108 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuAppliDisTrap
Processor performance overflow (CPU)	CPU value back below threshold	.1.3.6.1.4.1.31368.1.208 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuAppliDisEndTrap
Exceeding free space on disks	Disk memory exceeded	.1.3.6.1.4.1.31368.1.109 .iso.org.dod.internet.private.enterprises.systancia.applidis.diskAppliDisTrap
Exceeding free space on disks	Disk memory value back below threshold	.1.3.6.1.4.1.31368.1.209 .iso.org.dod.internet.private.enterprises.systancia.applidis.diskAppliDisEndTrap
Waiting list (CPU)	Waiting list size over threshold	.1.3.6.1.4.1.31368.1.130 .iso.org.dod.internet.private.enterprises.systancia.applidis.pqlTrap
Waiting list (CPU)	Waiting list size back below threshold	.1.3.6.1.4.1.31368.1.230 .iso.org.dod.internet.private.enterprises.systancia.applidis.pqlEndTrap
IIS pool activity	IIS pool recycled	.1.3.6.1.4.1.31368.1.131 .iso.org.dod.internet.private.enterprises.systancia.applidis.iisPoolTrap
System		
Application events observer	Number of errors or warnings per day	.1.3.6.1.4.1.31368.1.101 .iso.org.dod.internet.private.enterprises.systancia.applidis.appEventAppliDisTrap
Security events observer	Number of errors or warnings per day	.1.3.6.1.4.1.31368.1.102 .iso.org.dod.internet.private.enterprises.systancia.applidis.securEventAppliDisTrap
System events observer	Number of errors or warnings per day	.1.3.6.1.4.1.31368.1.103 .iso.org.dod.internet.private.enterprises.systancia.applidis.systemEventAppliDisTrap
TSE		
Availability of TSE	TSE not available	.1.3.6.1.4.1.31368.1.106

		.iso.org.dod.internet.private.enterprises.systancia.applidis.tseAppliDisTrap
Availability of TSE	TSE available	.1.3.6.1.4.1.31368.1.206 .iso.org.dod.internet.private.enterprises.systancia.applidis.tseAppliDisTrap
[Server]		
Availability of AppliDis servers	Server not available	.1.3.6.1.4.1.31368.1.104 .iso.org.dod.internet.private.enterprises.systancia.applidis.serverAppliDisTrap
Availability of AppliDis servers	Server available	.1.3.6.1.4.1.31368.1.204 .iso.org.dod.internet.private.enterprises.systancia.applidis.serverAppliDisTrap
[Services]		
Number of handles for the Application Server Service	Number of handles exceeded	.1.3.6.1.4.1.31368.1.110 .iso.org.dod.internet.private.enterprises.systancia.applidis.handlesApplicationTrap
Number of handles for the Application Server Service	Number of handles back below threshold	.1.3.6.1.4.1.31368.1.210 .iso.org.dod.internet.private.enterprises.systancia.applidis.handlesApplicationEndTrap
RAM consumption for the Application Server Service	RAM value exceeded	.1.3.6.1.4.1.31368.1.111 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramApplicationTrap
RAM consumption for the Application Server Service	RAM value back below threshold	.1.3.6.1.4.1.31368.1.211 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramApplicationEndTrap
CPU consumption for the Application Server Service	CPU value exceeded	.1.3.6.1.4.1.31368.1.112 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuApplicationTrap
CPU consumption for the Application Server Service	CPU value back below threshold	.1.3.6.1.4.1.31368.1.212 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuApplicationEndTrap
Application Server service state	Service stopped	.1.3.6.1.4.1.31368.1.113 .iso.org.dod.internet.private.enterprises.systancia.applidis.etatApplicationTrap
Application Server service state	Service started	.1.3.6.1.4.1.31368.1.213 .iso.org.dod.internet.private.enterprises.systancia.applidis.etatApplicationEndTrap
Number of handles for the Server Monitor Service	Number of handles exceeded	.1.3.6.1.4.1.31368.1.114 .iso.org.dod.internet.private.enterprises.systancia.applidis.handlesMonitorTrap
Number of handles for the Server Monitor Service	Number of handles back below threshold	.1.3.6.1.4.1.31368.1.214 .iso.org.dod.internet.private.enterprises.systancia.applidis.handlesMonitorEndTrap
RAM consumption for the Server Monitor Service	RAM value exceeded	.1.3.6.1.4.1.31368.1.115 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramMonitorTrap
RAM consumption for the Server Monitor Service	RAM value back below threshold	.1.3.6.1.4.1.31368.1.215 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramMonitorEndTrap
CPU consumption for the Server Monitor Service	CPU value exceeded	.1.3.6.1.4.1.31368.1.116 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuMonitorTrap
CPU consumption for the Server Monitor Service	CPU value back below threshold	.1.3.6.1.4.1.31368.1.216 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuMonitorEndTrap

Server Monitor service state	Service stopped	.1.3.6.1.4.1.31368.1.117 .iso.org.dod.internet.private.enterprises.systancia.applidis.etatMonitorTrap
Server Monitor service state	Service started	.1.3.6.1.4.1.31368.1.217 .iso.org.dod.internet.private.enterprises.systancia.applidis.etatMonitorEndTrap
Number of handles for the Server Redundancy Service	Number of handles exceeded	.1.3.6.1.4.1.31368.1.118 .iso.org.dod.internet.private.enterprises.systancia.applidis.handlesRedondeurTrap
Number of handles for the Server Redundancy Service	Number of handles back below threshold	.1.3.6.1.4.1.31368.1.218 .iso.org.dod.internet.private.enterprises.systancia.applidis.handlesRedondeurEndTrap
RAM consumption for the Server Redundancy Service	RAM value exceeded	.1.3.6.1.4.1.31368.1.119 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramRedondeurTrap
RAM consumption for the Server Redundancy Service	RAM value back below threshold	.1.3.6.1.4.1.31368.1.219 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramRedondeurEndTrap
CPU consumption for the Server Redundancy Service	CPU value exceeded	.1.3.6.1.4.1.31368.1.120 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuRedondeurTrap
CPU consumption for the Server Redundancy Service	CPU value back below threshold	.1.3.6.1.4.1.31368.1.220 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuRedondeurEndTrap
Server Redundancy service state	Service stopped	.1.3.6.1.4.1.31368.1.121 .iso.org.dod.internet.private.enterprises.systancia.applidis.etatRedondeurTrap
Server Redundancy service state	Service started	.1.3.6.1.4.1.31368.1.221 .iso.org.dod.internet.private.enterprises.systancia.applidis.etatRedondeurEndTrap
Number of handles for the Server Gateway Service	Number of handles exceeded	.1.3.6.1.4.1.31368.1.122 .iso.org.dod.internet.private.enterprises.systancia.applidis.handlesGatewayTrap
Number of handles for the Server Gateway Service	Number of handles back below threshold	.1.3.6.1.4.1.31368.1.222 .iso.org.dod.internet.private.enterprises.systancia.applidis.handlesGatewayEndTrap
RAM consumption for the Server Gateway Service	RAM value exceeded	.1.3.6.1.4.1.31368.1.123 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramGatewayTrap
RAM consumption for the Server Gateway Service	RAM value back below threshold	.1.3.6.1.4.1.31368.1.223 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramGatewayEndTrap
CPU consumption for the Server Gateway Service	CPU value exceeded	.1.3.6.1.4.1.31368.1.124 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuGatewayTrap
CPU consumption for the Server Gateway Service	CPU value back below threshold	.1.3.6.1.4.1.31368.1.224 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuGatewayEndTrap
Server Gateway service state	Service stopped	.1.3.6.1.4.1.31368.1.125 .iso.org.dod.internet.private.enterprises.systancia.applidis.etatGatewayTrap
Server Gateway service state	Service started	.1.3.6.1.4.1.31368.1.225 .iso.org.dod.internet.private.enterprises.systancia.applidis.etatGatewayEndTrap
Number of handles	Number of handles	.1.3.6.1.4.1.31368.1.126

for the IIS Service	exceeded	.iso.org.dod.internet.private.enterprises.systancia.applidis.handlesIISTrap
Number of handles for the IIS Service	Number of handles back below threshold	.1.3.6.1.4.1.31368.1.226 .iso.org.dod.internet.private.enterprises.systancia.applidis.handlesIISEndTrap
RAM consumption for the IIS Service	RAM value exceeded	.1.3.6.1.4.1.31368.1.127 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramIISTrap
RAM consumption for the IIS Service	RAM value back below threshold	.1.3.6.1.4.1.31368.1.227 .iso.org.dod.internet.private.enterprises.systancia.applidis.ramIISEndTrap
CPU consumption for the IIS Service	CPU value exceeded	.1.3.6.1.4.1.31368.1.128 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuIISTrap
CPU consumption for the IIS Service	CPU value back below threshold	.1.3.6.1.4.1.31368.1.228 .iso.org.dod.internet.private.enterprises.systancia.applidis.cpuIISEndTrap
IIS service state	Service stopped	.1.3.6.1.4.1.31368.1.129 .iso.org.dod.internet.private.enterprises.systancia.applidis.etatIISTrap
IIS service state	Service started	.1.3.6.1.4.1.31368.1.229 .iso.org.dod.internet.private.enterprises.systancia.applidis.etatIISEndTrap
Number of AppliDis licences used	Number of AppliDis licences used over threshold	.1.3.6.1.4.1.31368.1.132 .iso.org.dod.internet.private.enterprises.systancia.applidis.adisLicenceTrap
Number of AppliDis licences used	Number of AppliDis licences used back below threshold	.1.3.6.1.4.1.31368.1.232 .iso.org.dod.internet.private.enterprises.systancia.applidis.adisLicenceEndTrap
Virtual IP activity	The virtual IP has switch to another server	.1.3.6.1.4.1.31368.1.133 .iso.org.dod.internet.private.enterprises.systancia.applidis.adisVirtualIPSwapTrap
Virtual IP state	Virtual IP not available	.1.3.6.1.4.1.31368.1.134 .iso.org.dod.internet.private.enterprises.systancia.applidis.adisVirtualIPTrap
Virtual IP state	Virtual IP available again	.1.3.6.1.4.1.31368.1.234 .iso.org.dod.internet.private.enterprises.systancia.applidis.adisVirtualIPEndTrap

This list is available in the MIB definition downloadable from the SNMP monitoring administration page

(menu **Statistics -> Alarms -> Alarm distribution settings -> Export MIB**).

This .MIB file has to be compiled and integrated into the administration console used for network management (for example the NAGIOS tool).

List of AppliDis interrogations returned via SNMP

AppliDis allows the direct interrogation of various product parameters. These interrogations are made up of an OID identifier and a request result value. The OID syntax is standardized and is made up of a sequence of numbers separated by periods. Each AppliDis OID starts with the number sequence **.1.3.6.1.4.1.31368.1** corresponding to the **.iso.org.dod.internet.private.enterprises.systancia.applidis** identifier.

Note: In order to be able to carry out interrogations, the Microsoft SNMP service (included in Windows components) must be installed on the system executing the AppliDis administration server. Once installed, this service can be started or stopped from the AppliDis administration interface

The list of available requests is shown in the table below.

Information	Description	OID of the value
Database		
Backup database	Recovers database mode (main or backup)	.1.3.6.1.4.1.31368.1.5.2 .iso.org.dod.internet.private.enterprises.systancia.applidis .database.isSafeDatabase
Available database	Recovers the state of the database (available or not)	.1.3.6.1.4.1.31368.1.5.1 .iso.org.dod.internet.private.enterprises.systancia.applidis .database.isDatabaseContactable
Equipment		
Amount of RAM information	Number of servers returning information	.1.3.6.1.4.1.31368.1.7.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .ram.ramCount
Dedicated load limit	The dedicated load limit of server no. i	.1.3.6.1.4.1.31368.1.7.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .ram.ramChargeDedieeLimite.i
Total dedicated load	The total dedicated load of server no. i	.1.3.6.1.4.1.31368.1.7.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis .ram.ramChargeDedieeTotale.i
Physical memory available	Physical memory available on server no. i	.1.3.6.1.4.1.31368.1.7.3.i .iso.org.dod.internet.private.enterprises.systancia.applidis .ram.ramPhysiqueDispo.i
Total physical memory	Total physical memory on server no. i	.1.3.6.1.4.1.31368.1.7.4.i .iso.org.dod.internet.private.enterprises.systancia.applidis .ram.ramPhysiqueTotale.i
Percentage of physical memory free	Free physical memory on server no. i (in %)	.1.3.6.1.4.1.31368.1.7.5.i .iso.org.dod.internet.private.enterprises.systancia.applidis .ram.ramMemFreePercent.i
Amount of CPU information	Number of servers returning processor information.	.1.3.6.1.4.1.31368.1.8.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .cpu.cpuCount
Use of the processor (in %)	Use of the processor on server no. i	.1.3.6.1.4.1.31368.1.8.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .cpu.cpuPercentCPUUsed.i
Processor family	The family of the processor on server no. i	.1.3.6.1.4.1.31368.1.8.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis .cpu.cpuFamily.i

Information	Description	OID of the value
Processor frequency	The frequency of the processor on server no. i	.1.3.6.1.4.1.31368.1.8.3.i .iso.org.dod.internet.private.enterprises.systancia.applidis .cpu.cpuCurrentClockSpeed.i
Processor name	The name of server no. i	.1.3.6.1.4.1.31368.1.8.4.i .iso.org.dod.internet.private.enterprises.systancia.applidis .cpu.cpuServerName.i
Amount of disk information	Number of disks available.	.1.3.6.1.4.1.31368.1.9.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .disk.diskCount
Disk name	The name of disk no. i	.1.3.6.1.4.1.31368.1.9.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .disk.diskName.i
Disk size (in GB)	Size of disk no. i	.1.3.6.1.4.1.31368.1.9.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis .disk.diskSizeGo.i
Free disk space (in GB)	The space available on disk no. i	.1.3.6.1.4.1.31368.1.9.3.i .iso.org.dod.internet.private.enterprises.systancia.applidis .disk.diskFreeSpaceGo.i
Average free disk space (in GB)	The average space available on disk no. i	.1.3.6.1.4.1.31368.1.9.4.i .iso.org.dod.internet.private.enterprises.systancia.applidis .disk.diskFreeSpaceAverage.i
Servers sending CPU waiting list information	Number of servers sending CPU waiting list information	.1.3.6.1.4.1.31368.1.15.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .pql.pqlCount
CPU waiting list size for server n°i	Value of the waiting list size for server n°i	.1.3.6.1.4.1.31368.1.15.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .pql.pqlSize.i
Servers sending IIS pool recycling information	Number of servers sending IIS pool recycling information	.1.3.6.1.4.1.31368.1.16.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .iispool.iisPoolCount.i
IIS pool recycling information	Date of the last IIS pool recycling for the server n°i	.1.3.6.1.4.1.31368.1.16.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .iispool.iisPoolDate.i
System		
Amount of "Application Log" information	Number of servers returning "application log" information	.1.3.6.1.4.1.31368.1.1.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .appevent.appEventCount
Application errors	Counts the number of application errors which have occurred today on server no. i	.1.3.6.1.4.1.31368.1.1.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .appevent.appEventErrorCount.i
Application warnings	Counts the number of application warnings which have occurred today on server no. i	.1.3.6.1.4.1.31368.1.1.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis .appevent.appEventWarningCount.i

Information	Description	OID of the value
Amount of "Log Security" information	Number of servers returning "log security" information	.1.3.6.1.4.1.31368.1.2.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .securevent.appEventCount
Security Errors	Counts the number of security errors which have occurred today on server no. i	.1.3.6.1.4.1.31368.1.2.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .securevent.secureEventErrorCount.i
Security Warnings	Counts the number of security warnings which have occurred today on server no. i	.1.3.6.1.4.1.31368.1.2.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis .securevent.secureEventWarningCount.i
Amount of "Log System" information	Number of servers returning "log system" information	.1.3.6.1.4.1.31368.1.3.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .systemevent.systemEventCount
System errors	Counts the number of system errors which have occurred today on server no. i	.1.3.6.1.4.1.31368.1.3.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .systemevent.systemEventErrorCount.i
System Warnings	Counts the number of system warnings which have occurred today on server no. i	.1.3.6.1.4.1.31368.1.3.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis .systemevent.systemEventWarningCount.i
TSE		
Number of TSE sessions	Counts the total number of TSE sessions.	.1.3.6.1.4.1.31368.1.6.1 .iso.org.dod.internet.private.enterprises.systancia.applidis .tse.tseSessionCount
Number of inactive TSE sessions.	Counts the number of inactive TSE sessions.	.1.3.6.1.4.1.31368.1.6.2 .iso.org.dod.internet.private.enterprises.systancia.applidis .tse.tseDeadSessionCount
Server		
Number of servers	Counts the number of AppliDis servers	.1.3.6.1.4.1.31368.1.4.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .server.serverCount
Server name	The name of server no. i	.1.3.6.1.4.1.31368.1.4.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .server.serverName.i
Availability of the server	Is server no. i contactable?	.1.3.6.1.4.1.31368.1.4.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis .server.isServerContactable.i
Server role	The AppliDis role identifier of server no. i.	.1.3.6.1.4.1.31368.1.4.3.i .iso.org.dod.internet.private.enterprises.systancia.applidis .server.serverRoleID.i
Services		
Number of servers using Application Server service	Number of servers using Application Server service	.1.3.6.1.4.1.31368.1.10.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .application.applicationCount

Information	Description	OID of the value
Number of handles used by the Application service	Number of handles used by the Application service on server n°i	.1.3.6.1.4.1.31368.1.10.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .application.applicationHandles.i
RAM consumption for the Application Server Service	RAM consumption for the Application Server Service on server n°i	.1.3.6.1.4.1.31368.1.10.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis .application.applicationRAM.i
CPU usage for the Application Server Service	CPU usage for the Application Server Service on server n°i	.1.3.6.1.4.1.31368.1.10.3.i .iso.org.dod.internet.private.enterprises.systancia.applidis .application.applicationCPU.i
State of the Application Server service	State of the Application Server service on server n°i	.1.3.6.1.4.1.31368.1.10.4.i .iso.org.dod.internet.private.enterprises.systancia.applidis .application.applicationEtat.i
Number of servers using Server Monitor service	Number of servers using Server Monitor service	.1.3.6.1.4.1.31368.1.11.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .monitor.monitorCount
Number of handles used by the Server Monitor service	Number of handles used by the Monitor service on server n°i	.1.3.6.1.4.1.31368.1.11.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .monitor.monitorHandles.i
RAM consumption for the Server Monitor Service	RAM consumption for the Server Monitor Service on server n°i	.1.3.6.1.4.1.31368.1.11.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis .monitor.monitorRAM.i
CPU usage for the Server Monitor Service	CPU usage for the Server Monitor Service on server n°i	.1.3.6.1.4.1.31368.1.11.3.i .iso.org.dod.internet.private.enterprises.systancia.applidis .monitor.monitorCPU.i
State of the Server Monitor service	State of the Server Monitor service on server n°i	.1.3.6.1.4.1.31368.1.11.4.i .iso.org.dod.internet.private.enterprises.systancia.applidis .monitor.monitorEtat.i
Number of servers using Server Redundancy service	Number of servers using Server Redundancy service	.1.3.6.1.4.1.31368.1.12.0 .iso.org.dod.internet.private.enterprises.systancia.applidis .redondeur.redondeurCount
Number of handles used by the Server Redundancy service	Number of handles used by the Redundancy service on server n°i	.1.3.6.1.4.1.31368.1.12.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis .redondeur.redondeurHandles.i
RAM consumption for the Server Redundancy Service	RAM consumption for the Server Redundancy Service on server n°i	.1.3.6.1.4.1.31368.1.12.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis .redondeur.redondeurRAM.i
CPU usage for the Server Redundancy Service	CPU usage for the Server Redundancy Service on server n°i	.1.3.6.1.4.1.31368.1.12.3.i .iso.org.dod.internet.private.enterprises.systancia.applidis .redondeur.redondeurCPU.i
State of the Server Redundancy service	State of the Server Redundancy service on server n°i	.1.3.6.1.4.1.31368.1.12.4.i .iso.org.dod.internet.private.enterprises.systancia.applidis .redondeur.redondeurEtat.i

Information	Description	OID of the value
Number of servers using Server Gateway service	Number of servers using Server Gateway service	.1.3.6.1.4.1.31368.1.13.0 .iso.org.dod.internet.private.enterprises.systancia.applidis.gateway.gatewayCount
Number of handles used by the Server Gateway service	Number of handles used by the server Gateway service on server n°i	.1.3.6.1.4.1.31368.1.13.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis.gateway.gatewayHandles.i
RAM consumption for the Server Gateway Service	RAM consumption for the Server Gateway Service on server n°i	.1.3.6.1.4.1.31368.1.13.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis.gateway.gatewayRAM.i
CPU usage for the Server Gateway Service	CPU usage for the Server Gateway Service on server n°i	.1.3.6.1.4.1.31368.1.13.3.i .iso.org.dod.internet.private.enterprises.systancia.applidis.gateway.gatewayCPU.i
State of the Server Gateway service	State of the Server Gateway service on server n°i	.1.3.6.1.4.1.31368.1.13.4.i .iso.org.dod.internet.private.enterprises.systancia.applidis.gateway.gatewayEtat.i
Number of servers using IIS service	Number of servers using IIS service	.1.3.6.1.4.1.31368.1.14.0 .iso.org.dod.internet.private.enterprises.systancia.applidis.iis.iisCount
Number of handles used by the IIS service	Number of handles used by the IIS service on server n°i	.1.3.6.1.4.1.31368.1.14.1.i .iso.org.dod.internet.private.enterprises.systancia.applidis.iis.iisHandles.i
RAM consumption for the IIS Service	RAM consumption for the IIS Service on server n°i	.1.3.6.1.4.1.31368.1.14.2.i .iso.org.dod.internet.private.enterprises.systancia.applidis.iis.iisRAM.i
CPU usage for the IIS Service	CPU usage for the IIS Service on server n°i	.1.3.6.1.4.1.31368.1.14.3.i .iso.org.dod.internet.private.enterprises.systancia.applidis.iis.iisCPU.i
State of the IIS service	State of the IIS service on server n°i	.1.3.6.1.4.1.31368.1.14.4.i .iso.org.dod.internet.private.enterprises.systancia.applidis.iis.iisEtat.i
Maximum number of AppliDis licences	Maximum number of licences	.1.3.6.1.4.1.31368.1.17.1 .iso.org.dod.internet.private.enterprises.systancia.applidis.adisLicence.countMaxLicences
Number of AppliDis licences used	Number of licences used	.1.3.6.1.4.1.31368.1.17.2 .iso.org.dod.internet.private.enterprises.systancia.applidis.adisLicence.countUsedLicences
Number of AppliDis licences used	Number of licences left	.1.3.6.1.4.1.31368.1.17.3 .iso.org.dod.internet.private.enterprises.systancia.applidis.adisLicence.countAvailableLicences

This list is available in the MIB definition downloadable from the SNMP monitoring administration page

(menu **Statistics -> Alarms -> Alarm distribution settings -> Export MIB**).

This .MIB file has to be compiled and integrated into the administration console used for network management (for example the NAGIOS tool).

It should be noted that all these values are only accessible in read-only mode (SNMP-GET or SNMP-GETNEXT) and not in write mode (SNMP-SET). The values interrogated from the administration console cannot therefore be modified.

Interrogation requests must be executed on the SNMP protocol default port (port 161). This port is not configurable in AppliDis, unlike the port used to send alarm messages (SNMP-TRAP - port 162 by default).

Installation of the Microsoft SNMP Agent Service

The Microsoft SNMP extension agent has to be executed in order to be able to use SNMP with AppliDis. It must therefore be installed from the system components.

Note: If this SNMP extension agent is not installed, the sending of SNMP alarms will be **deactivated** in the AppliDis monitoring administration screen (shaded screen).

The SNMP service is not installed by default on the system and must be installed from the Add Windows Components screen:

Start - > Control panel - > Add / Remove Programs - > Add or Remove Windows Components.

The installation of the service is located under the heading "**Management and Analysis Tools**". Open this heading and check installation of the **SNMP** service.

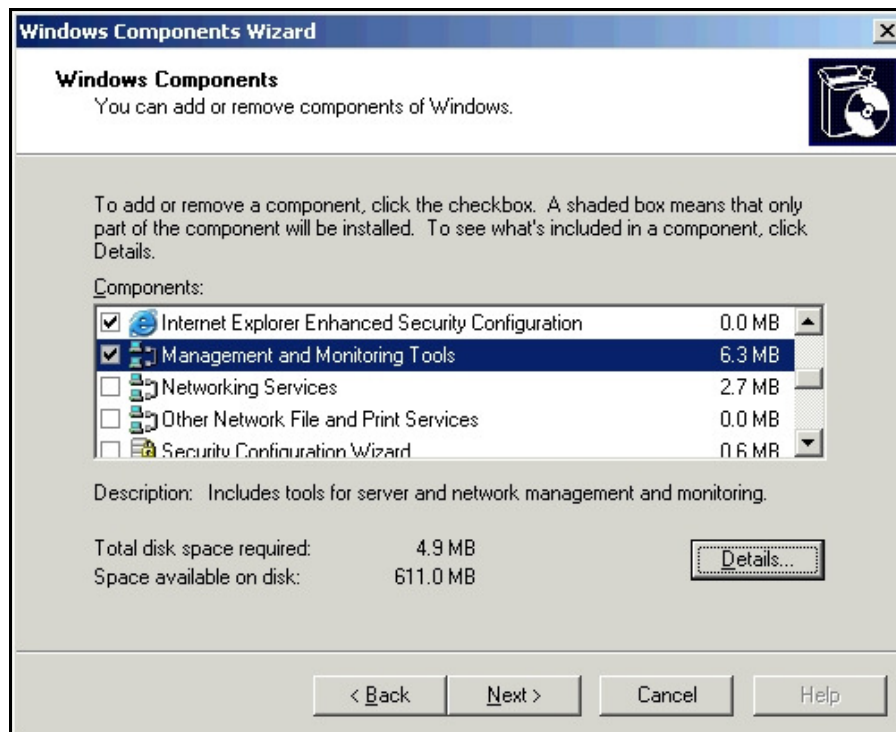


Figure 69 - Configuration of SNMP services.

The service will be configured automatically when AppliDis monitoring is started according to the information entered in the AppliDis SNMP alarm setting screen located on the administration site, in the following menu:

Monitoring->Alarms->Alarm transmission settings.

The service account has to be changed in the service called "SNMP service" by putting a domain administrator account in the Connection tab.

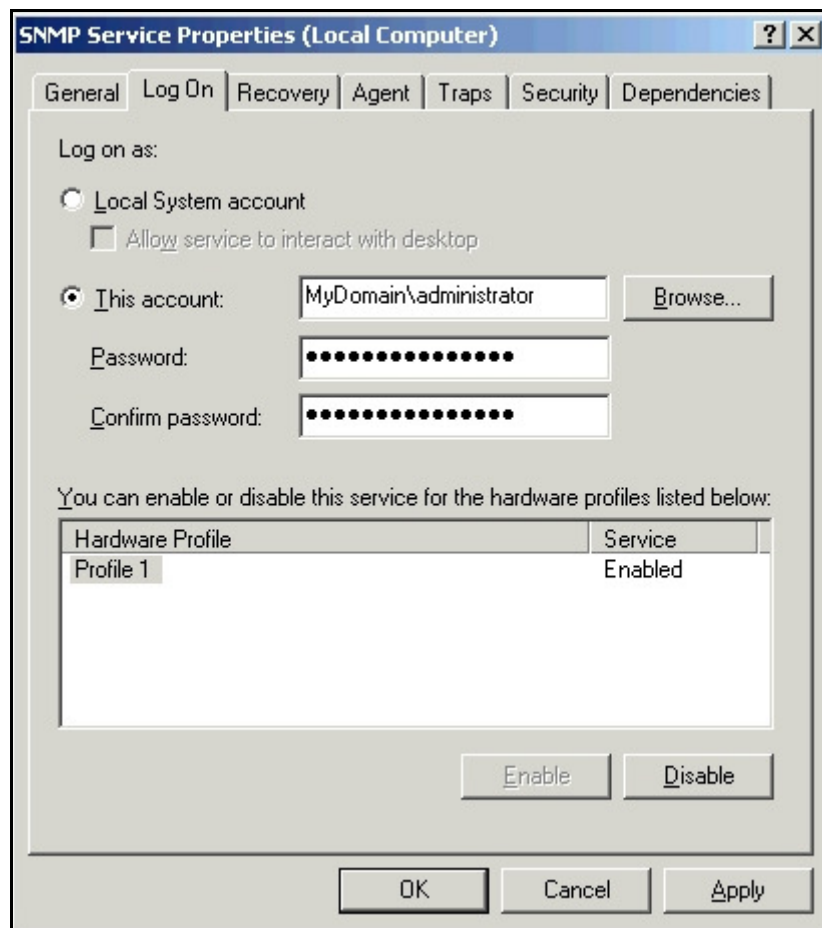


Figure 70 - SNMP service startup configuration

Menu: Configuration of the sending of AppliDis alarms via SNMP protocol

AppliDis SNMP alarms are configured in AppliDis administration, in the Monitoring -> Alarms -> Alarm transmission settings menu.

The configuration is executed via the screen shown below.

Note: If the SNMP extension agent service is not installed on the system, the sending of SNMP alarms is **deactivated** on this screen (shaded screen).

Figure 71 - Configuration of the SNMP manager

1. **Activation of Alarms by SNMP:** Allows the sending of SNMP alarms and SNMP interrogation requests to be activated or deactivated.
2. **SNMP IP manager:** Configures the IP address of the SNMP Manager to which the AppliDis monitoring tool will send SNMP alarms. Only this SNMP Manager will be authorized to execute SNMP requests on the AppliDis agent.
3. **Port:** The network port used to send SNMP alarms (SNMP-TRAP - 162 by default). Requests (GET/GETNEXT/SET) must use port 161.
4. **Community:** The SNMP community used to send SNMP alarms (traps) and for interrogation requests from the SNMP Manager (since the community is generally public or private).
5. **OID prefix:** SNMP identifier (Object ID), in digital format, representing the AppliDis OID. All alarms and parameters that can be interrogated will start with this OID (= .iso.org.dod.internet.private.enterprises.systancia.applidis in text format). This field is displayed on a purely informative basis and cannot be parameterized.
6. **Activation of the AppliDis SNMP agent:** Allows the system extension agent service to be stopped or started. If this extension agent is deactivated, the SNMP Manager will no longer be able to execute requests to the AppliDis agent. However, the sending of alarms will remain active as long as the "Activation of alarms by SNMP" box above remains checked.
7. **Export MIB:** Allows the file of variable and alarm definitions proposed by AppliDis SNMP to be downloaded. This file is to be integrated into the SNMP Manager used.

25 Viewing the statistics

The administrator can use the statistics to see which applications are most used or which servers are most requested, which applications are launched, by whom and for how long. You will find all these answers in the statistics.

25.1 Installing the Macromedia Shockwave plug-in

Some presentations are based on piechart-style graphics. Macromedia's Shockwave plugin must be downloaded before they can be viewed. You are automatically prompted to install this plugin when accessing pages which require it. If your Internet Explorer security settings prevent you from downloading this plugin, you must carry out the following steps:

1. Launch Internet Explorer.
2. Go to Tools, then Internet Options.
3. Select the Security tab.
4. Select Trusted sites and then click then on the Sites button
5. Add the site <http://download.macromedia.com> to the sites in this zone.
6. Confirm your selection by clicking on OK.

Note: The periods of use shown in the statistics do not take into account the application disconnection time. Thus if a user executes the Word application via AppliDis at 15:00:00, disconnects the application at 15:05:00 and returns to the application at 15:10:00 to close it definitively at 15:15:00, a start date of 15:00:00 and a closing date of 15:15:00 will be displayed for a duration of 00:10:00.

25.2 Statistics summaries

These summaries present the use of AppliDis since its installation (total number of launched sessions, total application usage time, usage averages, etc.)

You are also given daily statistics by server, by user, by application, etc.

Viewing the statistics for the day

Uses on the day in progress are shown in the statistics classified by application, by server or by user.

1. Click on Statistics in the main menu. By default you will be in the Summaries sub-menu and, the Statistics for the day icon will be activated on the page.
2. The list of applications launched during the day will then be displayed
3. Click on one of the three buttons: Servers today, Applications today, Users today in order to have a closer examination of the use of AppliDis on the current day. These three buttons will take you to the pages described further on in this section "Viewing the statistics" under the titles "By server", "By application" and "by user" with the time range pre-set to the current day.

Viewing the general summary

The general summary gives a brief overview of some general information since the installation of AppliDis:

- total number of applications launched.
- total time of use.
- date of first launch, date of last launch.
- average number of launches per day.
- average period of use per application.

1. Click on Statistics in the main menu. By default you will be in the Summaries sub-menu.
2. Click on the Summaries icon to display the general summary.

Viewing the statistics summary for a user

1. Click on Statistics in the main menu. By default you will be in the Summaries sub-menu.
2. Click on the Summaries icon.
3. Select the user for whom you wish to obtain a summary of use.
4. Click on Display.

Viewing the statistics summary for an application

1. Click on Statistics in the main menu. By default you will be in the Summaries sub-menu.
2. Click on the Summaries icon.
3. Select the application for which you wish to obtain a summary of use.
4. Click on Display.

Viewing the statistics summary for a server

1. Click on Statistics in the main menu. By default you will be in the Summaries sub-menu.
2. Click on the Summaries icon.
3. Select the server for which you wish to obtain a summary of use.
4. Click on Display.

25.3 Statistics by Server

You can see the statistics sorted on a per-server basis, such as:

- the distribution of the period of use by server.
- the distribution of users by server ("Who is connecting to my server?").
- the distribution of applications by server ("Which are the most highly-used applications on my server?").

These statistics specify use (in duration or in number of runs) for each server per hour, per day and per month.

Viewing the use of servers

1. Click on Statistics in the main menu.
2. Go to the By Server sub-menu.
3. Select another server or All from the Server list to display the statistics of another server or all the servers.
4. Select either duration to display the period of use of the selected server, or number of executions to display the number of times that this server was requested, from the Display list.
5. Select Yearly from the Period list to obtain the full statistics over one year, detailed per month. You can then determine the year by modifying the value of the Year list.
6. Select Monthly from the Period list to obtain the full statistics over one month, detailed per day. You can determine the month and the year by modifying the values of the Month lists. It is also possible to obtain a monthly value from the yearly display, by clicking on the graphic bar for which you wish to have precise details.
7. Select Daily from the Period list to obtain the full statistics over one day, detailed per hour. You can determine the day by clicking on the Day button. It is also possible to obtain a daily value from the monthly display, by clicking on the graphic bar for which you wish to have precise details.
8. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

Note: In the various detailed tables available in the statistics, it is possible to sort information according to each column heading, in ascending or descending order, simply by clicking on the heading.

Viewing the memory and CPU usage of a server

The mean values of usage according to the days of the week can be obtained by viewing this information. Thus you will be able to see the CPU usage of a particular server for each Monday, for example. The graph shows each hour of the day in 15 minute segments. The legend specifies the total mean value and the maximum value reached.

1. Click on Statistics in the main menu.
2. Go to the By Server sub-menu.
3. Click on the Memory and CPU usage icon.
4. Select the CPU or Memory value from the Characteristics list to obtain the statistics of the average usage of the processor (CPU) or the average usage of the memory.
5. Select another server or All from the Server list to display the statistics of another server or all the servers.
6. Select a day from the Day list to find out its usage.

Viewing the distribution of server use

This information provides details on how the load balancing function will distribute the applications and users on the servers. Information is available on both duration and number of uses. By default, information is displayed in graphic format.

1. Click on Statistics in the main menu.
2. Go to the By Server sub-menu.
3. Click on the Use distribution icon.
4. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
5. In the Display list, you can change the type of data displayed, i.e. either duration or number of runs.
6. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

Viewing user distribution for servers

Viewing the distribution of users for servers makes it possible to note how the users requested the servers. Information is available on both duration and number of uses. By default, information is displayed in graphic format.

1. Click on Statistics in the main menu.
2. Go to the By Server sub-menu.
3. Click on the User Distribution icon.
4. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
5. In the Display list, you can change the type of data displayed, i.e. either duration or number of runs.
6. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

Viewing application distribution for servers

Viewing the distribution of applications for the servers makes it possible to note how the applications are distributed on the various servers. This information can be particularly important for critical applications, the execution of which is monitored. Information is available on both duration and number of uses. By default, information is displayed in graphic format.

1. Click on Statistics in the main menu.
2. Go to the By Server sub-menu.
3. Click on the Application distribution icon.
4. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
5. In the Display list, you can change the type of data displayed, i.e. either duration or number of runs.
6. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

25.4 Statistics by application

This section makes it possible to display the classification of uses by applications. Information includes the time of use of each application, the number of times each application is launched, the classification of users by application (in other words "who uses this application?"), and lastly the distribution of launches per server for a given application (in other words "where was this application launched?").

Viewing the use of applications

Viewing the use of the applications makes it possible to obtain the statistics of use, with regard to both duration and number of uses, for all the applications or for a particular application. By default, information is displayed in graphic format.

1. Click on Statistics in the main menu.
2. Go to the By application sub-menu.
3. Select another application or All from the Application list to display the statistics of another application or all the applications.
4. Select from the Display list either duration to display the period of use of the selected application, or number of runs to display the number of times that this application was executed.
5. Select Yearly from the Period list to obtain the full statistics over one year, detailed per month. You can then determine the year by modifying the value of the Year list.
6. Select Monthly from the Period list to obtain the full statistics over one month, detailed per day. Then determine the month and the year by modifying the values of the Month lists. It is also possible to obtain a monthly value from the yearly display, by clicking on the graphic bar for which you wish to have precise details.
7. Select Daily from the Period list to obtain the full statistics over one day, detailed per hour. Then determine the day by clicking on the Day button. It is also possible to obtain a daily value from the monthly display, by clicking on the graphic bar for which you wish to have precise details.
8. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.



Figure 72 - Example of display of the use of an application over a year.

Viewing the distribution of use for applications

This information shows which are the most commonly used applications in your AppliDis server cluster.

1. Click on Statistics in the main menu.
2. Go to the By application sub-menu.
3. Click on the Use distribution icon.
4. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
5. In the Display list, change the type of data displayed, i.e. either duration or number of runs.
6. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

Viewing user distribution for applications

Viewing the distribution of users for applications makes it possible to note the applications requests by users. Information is available on both duration and number of uses. By default, information is displayed in graphical format.

1. Click on Statistics in the main menu.
2. Go to the By application sub-menu.
3. Click on the User Distribution icon.
4. Select another application or All from the Application list to display the statistics of another application or all the applications.
5. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
6. In the Display list, change the type of data displayed, i.e. either duration or number of runs.
7. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

Viewing the distribution of servers for applications

Viewing the distribution of servers for applications makes it possible to note how the applications are distributed among the various servers. This information can be particularly important for critical applications the execution of which is monitored. Information is available on both duration and number of uses. By default, information is displayed in graphical format.

1. Click on Statistics in the main menu.
2. Go to the By application sub-menu.
3. Click on the Server distribution icon.
4. Select another application or All from the Application list to display the statistics of another application or all the applications.
5. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
6. In the Display list, change the type of data displayed, i.e. either duration or number of runs.
7. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

25.5 Statistics by user

This section makes it possible to see the classification of uses by user. Information includes the time of use of each user, the number of launches by each user, the users who consume the most in terms of launches or time of use, the distribution by server for a given user ("On which server does this user spend the most time?" or "On which server does this user launch the most applications?") and finally which applications are launched the most or are most used in terms of time for a given user ("Which applications does my user use the most?").

Viewing use by user

1. Click on Statistics in the main menu.
2. Go to the By user sub-menu.
3. Select another user or All from the User list to display the statistics of another user or all the users.
4. Select from the Display list either duration to display the period of use of the selected application, or number of runs to display the number of times that this application was executed.
5. Select Yearly from the Period list to obtain the full statistics over one year, detailed per month. Then determine the year by modifying the value of the Year list.
6. Select Monthly from the Period list to obtain the full statistics over one month, detailed per day. Then determine the month and the year by modifying the values of the Month lists. It is also possible to obtain a monthly value from the yearly display, by clicking on the graphic bar for which you wish to have precise details.
7. Select Daily from the Period list to obtain the full statistics over one day, detailed per hour. Then determine the day by clicking on the Day button. It is also possible to obtain a daily value from the monthly display, by clicking on the graphic bar for which you wish to have precise details.
8. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.



Figure 73 - Example of display of the use distribution of the various users.

Viewing the use distribution for users

This information shows which users are most regularly making use of your AppliDis server cluster.

1. Click on Statistics in the main menu.
2. Go to the By user sub-menu.
3. Click on the Use distribution icon.
4. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
5. In the Display list, change the type of data displayed, i.e. either duration or number of runs.
6. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

Viewing the server distribution for users

Viewing the distribution of servers for users makes it possible to note how the users are distributed on the various servers. This information can be useful during maintenance periods, in order to see which users would be most affected by the stopping of a server (if there is no redundancy of applications on another AppliDis application server).

1. Click on Statistics in the main menu.
2. Go to the By user sub-menu.
3. Click on the Server distribution icon.
4. Select another user or All from the User list to display the statistics of another user or all the users.
5. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
6. In the Display list, change the type of data displayed, i.e. either duration or number of runs.
7. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

Viewing the use distribution for users

Viewing the distribution of applications for users makes it possible to note how the applications are distributed for the various users. This information enables you to know which applications are actually executed by your users from the range available to them.

1. Click on Statistics in the main menu.
2. Go to the By user sub-menu.
3. Click on the Application distribution icon.
4. Select another user or All from the User list to display the statistics of another user or all the users.
5. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
6. In the Display list, change the type of data displayed, i.e. either duration or number of runs.
7. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

25.6 Statistics by desktop

This section makes it possible to display the classification of uses by desktops. Here you will find usage time for each desktop, the number of launches for each desktop, the distribution of users by desktop (in other words, "who is using this desktop?"), and lastly the distribution of launches per server for a given desktop (in other words, "where was this desktop launched?").

Viewing the use of desktops

Viewing the use of the desktops makes it possible to obtain the statistics of use, with regard to both duration and number of uses, for all the desktops or for a particular desktop. By default, information is displayed in graphic format.

1. Click on Statistics in the main menu.
2. Go to the By desktop sub-menu.
3. Select another desktop or All from the Desktop list to display the statistics of another desktop or all the desktops.
4. Select either duration to display the period of use of the selected desktop, or number of executions to display the number of times that this desktop was executed, from the Display list.
5. Select Yearly from the Period list to obtain the full statistics over one year, detailed per month. You can then determine the year by modifying the value of the Year list.
6. Select Monthly from the Period list to obtain the full statistics over one month, detailed per day. Then determine the month and the year by modifying the values of the Month lists. It is also possible to obtain a monthly value from the yearly display, by clicking on the graphic bar for which you wish to have precise details.
7. Select Daily from the Period list to obtain the full statistics over one day, detailed per hour. Then determine the day by clicking on the Day button. It is also possible to obtain a daily value from the monthly display, by clicking on the graphic bar for which you wish to have precise details.
8. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

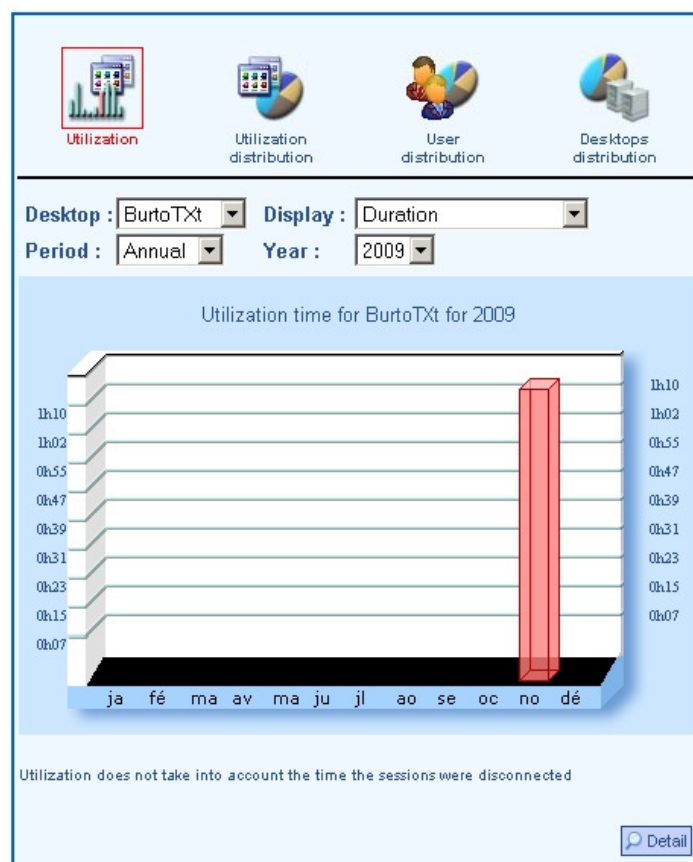


Figure 74 - Example of display of the use of an desktop over a year.

Viewing the use distribution for desktops

This information shows which are the most commonly used desktops in your AppliDis server cluster.

1. Click on Statistics in the main menu.
2. Go to the By desktop sub-menu.
3. Click on the Use distribution icon.
4. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
5. In the Display list, change the type of data displayed, i.e. either duration or number of runs.
6. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

Viewing user distribution for desktops

Viewing the distribution of users for desktops makes it possible to note the desktop requests by users. Information is available on both duration and number of uses. By default, information is displayed in graphic format.

1. Click on Statistics in the main menu.
2. Go to the By desktop sub-menu.
3. Click on the User Distribution icon.
4. Select another desktop or All from the Desktop list to display the statistics of another desktop or all the desktops.
5. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
6. In the Display list, change the type of data displayed, i.e. either duration or number of runs.
7. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

Viewing the server distribution for desktops

Viewing the distribution of servers for desktops makes it possible to note how the desktops are distributed among the various servers. This information can be particularly important for critical desktops the execution of which is monitored. Information is available on both duration and number of uses. By default, information is displayed in graphical format.

1. Click on Statistics in the main menu.
2. Go to the By desktop sub-menu.
3. Click on the Server distribution icon.
4. Select another desktop or All from the Desktop list to display the statistics of another desktop or all the desktops.
5. From the Period list, select the period for which the distribution is calculated: Today, Current week, Current month, Current year, All statistics.
6. In the Display list, change the type of data displayed, i.e. either duration or number of runs.
7. Click on the Detail button to obtain the table equivalent to the displayed graph, regardless of the settings.

25.7 Search in the statistics

The search tool is used to find all the applications launched over a given period by applying and combining several types of filters (for a given server, for a given application, for a given desktop, for a given user). Moreover, it allows the export of these results to a file in .csv format (the data are separated by commas)

Generate a new search in the statistics

1. Click on Statistics in the main menu.
2. Go to the Search sub-menu.
3. Click on the search start date and search end date buttons to select the time range of the search.
4. If you select a particular server (by selecting its name instead of "all") the search will be limited to this server. The same applies for applications or desktops and users. You can also use a combination of these filters (for example a given user for a given server).
5. When you have set all your search choices, click on Search.
6. The search result will be displayed in a list. By default, this list is classified by the close date of the application or desktop. Change the classification by clicking on the column headings (for example, if you click on Users, you will obtain a classification according to the names of users in alphabetical order. Click on the same column twice (for example on Users again) to display the list in reverse order (in our example this will be in reverse alphabetical order: from Z to A).

Exporting the search results to a .csv file

1. Click on Statistics in the main menu.
2. Go to the Search sub-menu.
3. Click on the search start date and search end date buttons to select the time range of the search.
4. If you select a particular server (by selecting its name instead of "all") the search will be limited to this server. The same applies for applications, desktops and users. You can also use a combination of these filters (for example a given user for a given server).
5. When you have set all your search choices, click on Search.
6. The search result will then be displayed.
7. Click on Export CSV.
8. A dialog box called Downloading files will open.
9. Click on Save and select the location where you want to save the file.

26 Printing

With the AppliDis printing module, a number of print server features can be configured:

- a universal printer,
- a universal session printer,
- or network printers.

26.1 Print format

The AppliDis universal printer handles the following print formats:

- RAW
- TEXT
- as well as the Microsoft EMF format.

This applies both to the server's common universal printer and to the "hot-mounted" universal printers specific to individual sessions.

To print a document in a Microsoft Windows environment, an application may perform this operation:

- either via the Microsoft print spooler (which accounts for the majority of cases, sending documents in EMF for Windows format to the printer),
- or printing by invoking the printer driver (directly or not) via the print spooler. This type of printing may be performed either in text or RAW format. At that point, all of the commands for generating the print job in question are sent by the application itself.

This method of printing is still used by 16-bit Windows applications and also by some applications under the Unix architecture.

26.2 Universal printer configuration

The AppliDis universal printer is configured directly from the AppliDis Administration console, in the Print/universal printer menu. You can thus parameterize the print options and set the rate of flow transfer according to your clients' LAN/WAN zone. By default, the AppliDis universal printer is deactivated.

Activating the universal driver

1. Click on Print in the main menu. Go to the Universal Printer sub-menu.
2. Check the Activation of the universal printer on the Application servers box.
3. Check the desired options, adjust the default band-width and the type of compression required.
4. Click on OK to save the modifications.

26.3 Print options

The following parameter setting options are available:

Activating resumption of work after printing

When this option is active, in the event of an interruption in the client-server connection, the print job will be stored in a buffer memory of the session.

Activating display of the progress bar when sending data

Displays the printing data progress bar on the user's screen.

Activate compression

Specification of the algorithm of compression for print data. AppliDis Fusion 4 implements the ZIP, RLE32 and ZLib algorithms.

Limiting data transfer rate

This makes it possible to limit the default transfer rate of the data between the client and the server.

26.4 Parameter setting of the transfer rates according to client zones

The transfer rate management interface enables you to assign specific rates to each of your clients' IP zones.

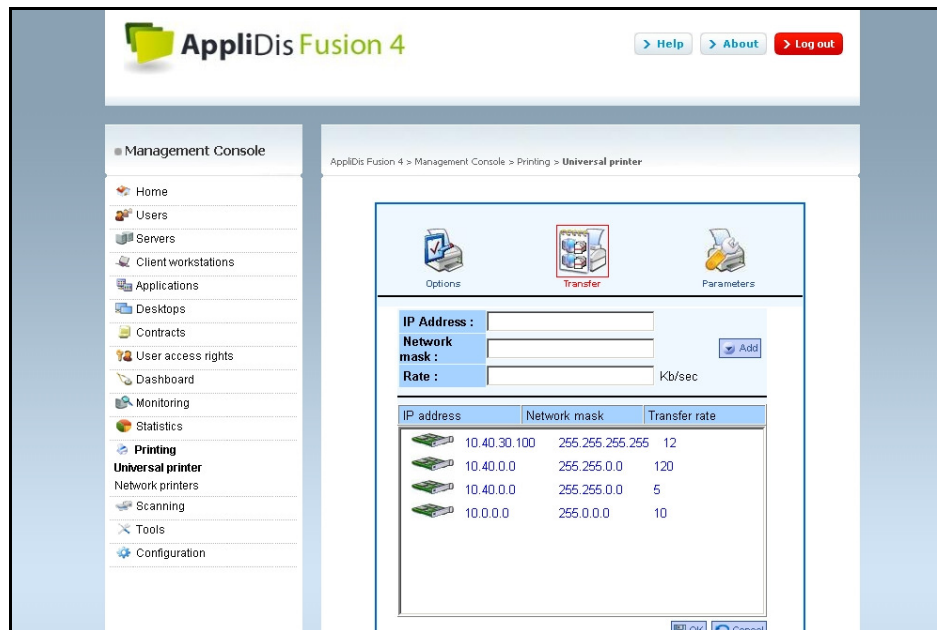


Figure 75 - Parameter setting of transfer rates according to IP zone

This method of IP management is intended for clients in WAN environments.

Configuring zones

Specify the various zones (or network maps) for which you wish to assign a transfer rate. The configuration settings located at the top of the list have priority.

Once a zone is placed in the list, you can select it and then increase or decrease its priority.

The transfer rate specified in this list always takes priority over the default transfer rate specified in the print options.

26.5 Dedicated universal printer per named session

With a dedicated universal printer per named session, a universal printer can be created for each session open on the application servers and Windows desktop servers, creating a universal printer for each connected user.

With the universal printer, each AppliDis applications server has access to a unique printer named "AppliDis Universal Printer". Each print request from a server to this universal printer is processed and redirected to the corresponding session, based on the name of the document. Each document is marked for being sent on to the session requesting the print operation. This marking consists of:

- the identifier for the session in which the print request was made,
- the user's login.

This is necessary to ensure the print jobs are sent to the correct Microsoft TSE/RDS session. The identifiers enable the creation of a temporary storage area in the nominated print spooler.

However, this approach suffers from a number of limitations:

- The documents need to be marked with the session identifier before the print request is actually made in the Microsoft TSE/RDS session; if they are not, the document will not be marked and therefore will not be processed. This can happen, for example, if an application is launched using the "print" command to create a direct print (e.g. a right-click on a Word document followed by selection of the "Print" command in the context menu). In this case, the print request is handled by the Microsoft Windows operating system ahead of all other programs.
- The print request must be made directly by a program from the session. In cases where a program attempts to perform a print operation by sending the name of the target printer to a program from another session (e.g. a service whose purpose is to generate print jobs), the print job will actually be handled by the other session (in which case the session ID marking information will either be lost or will not match the original session). Furthermore, in this case, user details will no longer be those of the user who issued the print request (e.g. for a service, the effective username will be the name associated with the account running the service).

In order to overcome these limitations, the 'dedicated universal printer per named session' mechanism was introduced to generate a universal printer dedicated to the user's Microsoft Terminal Server session. This printer is visible only to the user in question (and to administrators). The name of this printer contains all necessary identifiers for marking print jobs. This marking may include (per configuration) a combination of the following information: session ID, user name, server name. The name of this printer must contain at least the session ID. If the printer name has not been configured to contain the user name, the printer name will contain the name of the user sending the print job, in the same way as for the common universal printer for an application server.

Additional options for the graphical interface

To control this new functionality for the universal printer, the graphical interface has been improved on the AppliDis administration console in:

Print menu / Universal Printer, "Settings" tab, where various options can be configured, including automatic mounting of a dedicated universal printer for the TSE session.

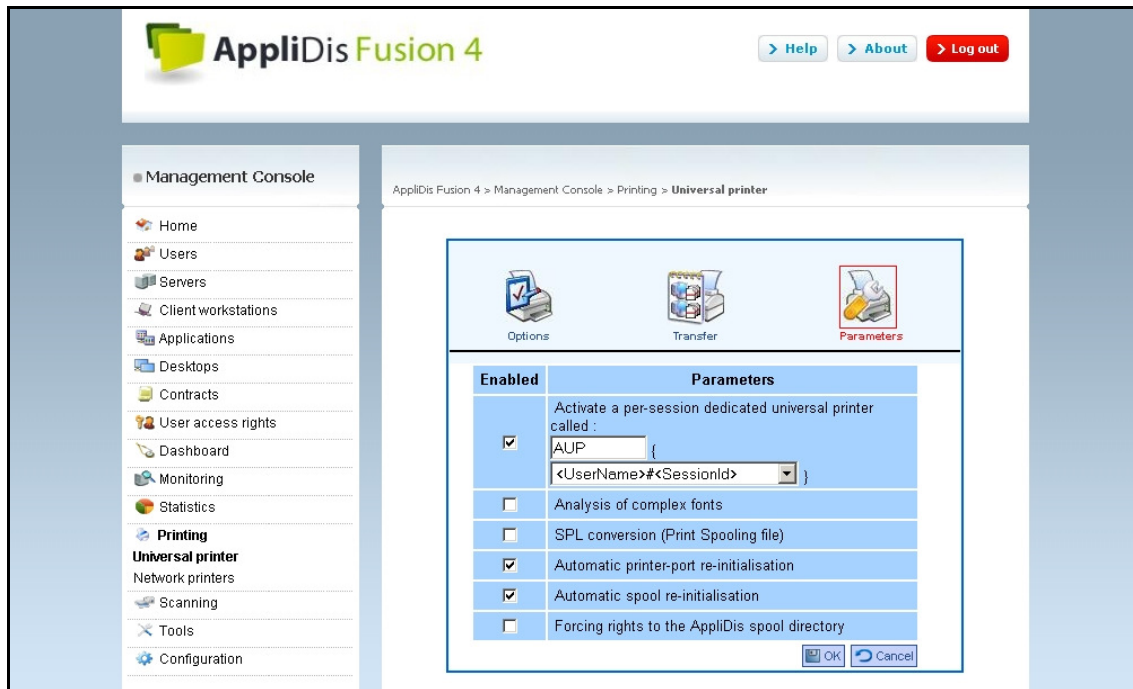


Figure 76 - Options for automatically mounting a universal printer

Checking the "Activate a dedicated universal printer per named session" box will place a dedicated universal printer for each AppliDis session on all application servers.

You can also use this interface to configure the IDs and names of the associated printers for the sessions.

The "Analyze complex fonts" checkbox allows you, if desired, to activate the analysis of fonts with a font name which differs from the name of the file containing the actual font.

The "SPL (Print Spooling File) conversion" checkbox allows you, if desired, to activate the server-side conversion of Microsoft-reserved EMF instructions.

The "Automatically re-initialize printer port" checkbox allows you, if desired, to activate automatic flushing of the AppliDis universal printer ports.

The "Automatically re-initialize spooler" checkbox allows you, if desired, to automatically clean out SID_No. directories for the session storing the jobs.

The "Force AppliDis spool directory privileges" checkbox allows you, if desired, to activate control over privileges and to reset them if they are incorrect for the user.

26.6 Printing with the Universal printer

The AppliDis universal printer is seen on the server as an additional printer. It is automatically managed by AppliDis. No specific installation is necessary on the client workstation.

Selecting the Universal printer

When users select the "Print" menu from their application, the dialog box below opens (**Erreur ! Source du renvoi introuvable.**), displaying the various available printers. To print to a printer from the client desktop via the AppliDis universal printer, just select "AppliDis Universal Printer" as the printer. If this printer is set as the default printer and users select the "Direct Print" menu from their application, the application will print without displaying this dialog box.

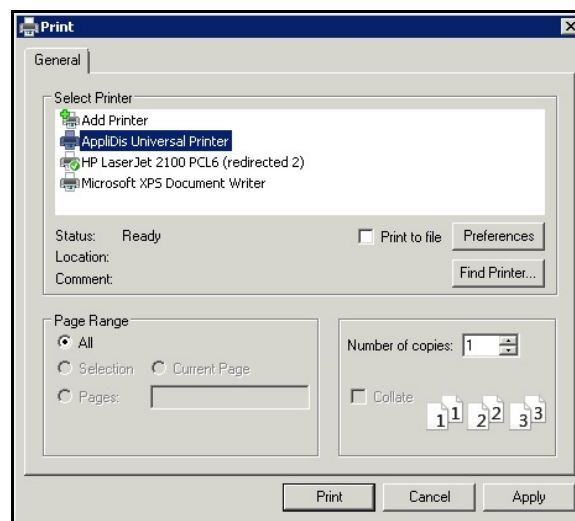


Figure 77 - Printer selection box on the server

Note: The universal printer manages the selection of pages to be transferred. Example: if you only want to print pages 2 to 10 of a 500-page document, this can be specified in the interface shown above. In this way, only 9 pages will be sent to the client workstation.

Selecting the client workstation printer

After transferring print data onto the client, the box to select the workstation printer will be displayed. The user will then select his printer from all those present on the client workstation, as well as the various properties (Feed, Recto-Verso, etc.).

26.7 Network printer filtering

One of the issues when using network printers within an application publishing product is the rapidly-growing list of network printers which can be seen by users.

AppliDis has a function which enables network printers to be filtered by geographical location of users.

Activating network printer filtering

1. Click on Print in the main menu. Go to the Network Printers sub-menu.
2. Check the box: Activate network printer access filtering.
3. Check the "Hide network printers inherited from Terminal Server / Remote Desktop Service" box if you do not wish to see these printers

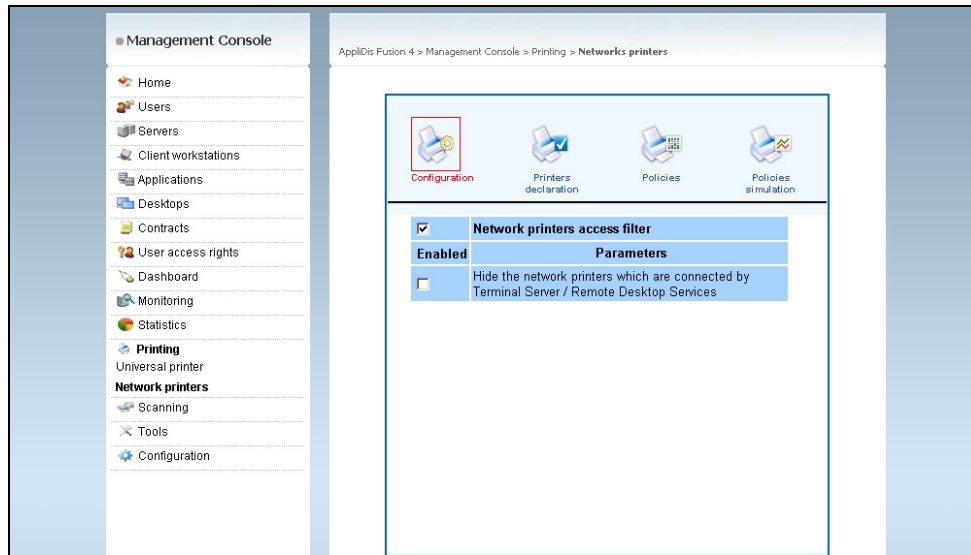


Figure 78 - Activating network printer access filtering

Declaring printers and implementing a filtering strategy

The filtering system is based on two components :

1. The first relates to the declaration of printers within the scope of the server environment.

Using a list provided by the console, you must specify which printers can subsequently be governed by a specific strategy.

2. The second component is the creation of a strategy for linking declared network printersto ranges of IP addresses associated with users. A strategy is defined by a range of IP addresses and a list of network printers with one printer from the list which may be defined as a default printer. All users accessing AppliDis from inside this IP address range will have native access to these printers, and will be assigned the specified default printer.

There is an option for testing strategies you have created: inserting an IP address for the client desktop will give you a list of the network printers visible to the user based on the strategies applicable to that user.

Note : Before using this AppliDis functionality, network print drivers must be installed on all application servers. This operation will have to be carried out using an account with Administrative rights.

Also check that the driver is compatible according to your server, for example for a Windows Server 2008 R2, the driver of the network printer must be compatible 64-bit

27 Scanning

The AppliDis scanning module enables users to operate scanning peripherals with their published applications or desktops. These peripherals may be cameras, scanners or any other TWAIN-compliant devices. This module only works on Windows Server 2003 x86 and x64.

27.1 Generic peripherals

AppliDis defines a generic peripheral as one whose name you can configure (the default name being "AppliDis ezScan"). Users wishing to scan a document must select a source. The generic peripheral in question will appear on the list of sources appearing in the published TWAIN-compliant application. The user will need to select this peripheral to gain access to the sources on his/her workstation, and thus the scanner attached to the workstation or the camera connected to a USB port on that machine.

27.2 Activating scanning

2. Click on Scanning in the main menu.
3. If you wish to, change the name which appears as the "source" to be selected for users in the "Name of peripheral", "Type of peripheral", "Name of peripheral manufacturer" fields.
4. Check the Activation of remote scanning on the Application servers box.
5. As for the universal printer, you can alter the settings for using scans, including bandwidth and compression.

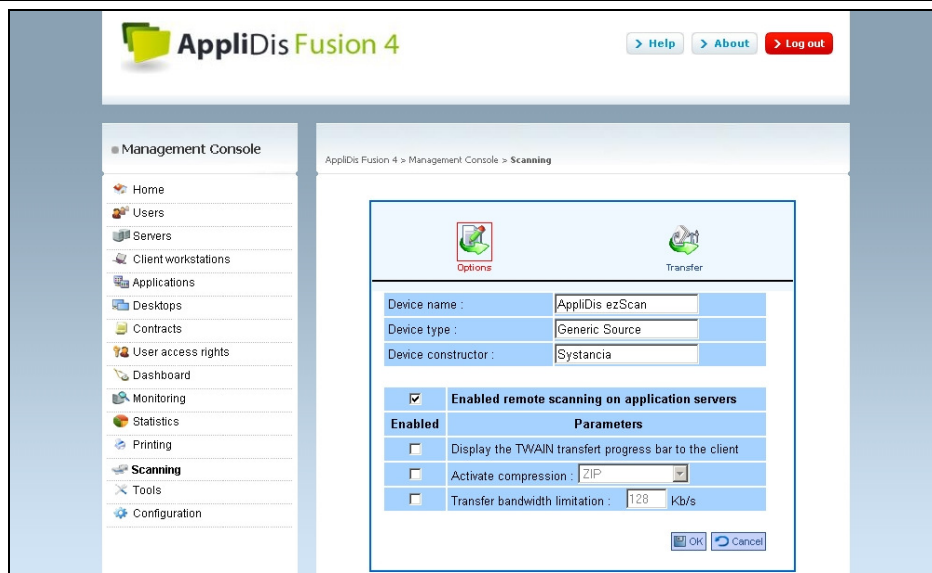


Figure 79 - Activating scanning

27.3 Parameter setting of transfer rates according to client zones

The transfer rate management interface enables you to assign specific rates to scanning in each of your clients' IP zones.

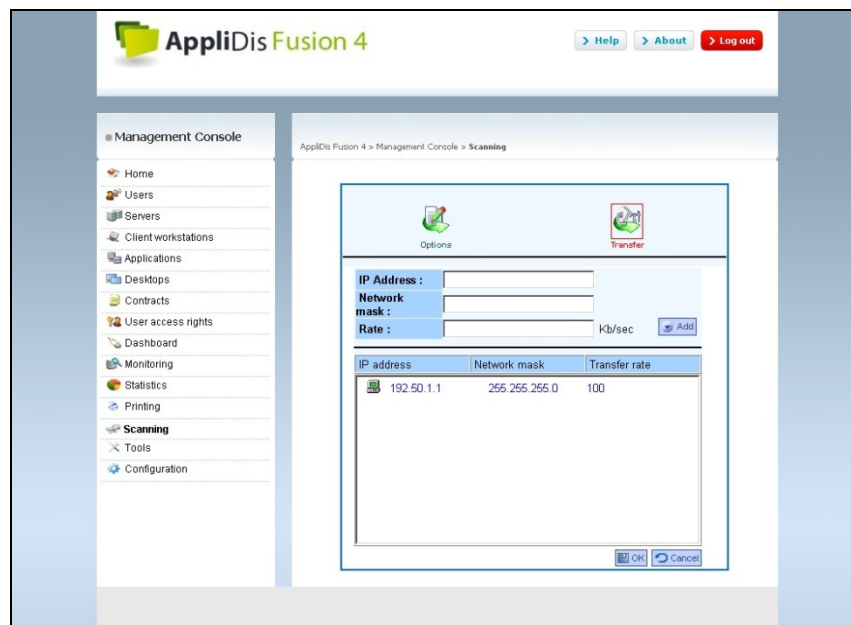


Figure 80 - Parameter setting of transfer rates according to IP zone

This method of IP management is intended for clients in WAN environments.

28 AppliDis delegated administration

The administrator can manage several delegated administration profiles from the AppliDis administration console.

28.1 Adding a delegated administration group/OU

1. Click on the Configuration menu, then on the Administrators sub-menu.
2. Click on Add group to add a group (Add Organizational Unit to add OUs).
3. Select the groups/OUs present in AppliDis in the list on the left and add them to the list on the right by clicking on the right arrow.
4. Click on OK to return to the Configuration/Administrators page.

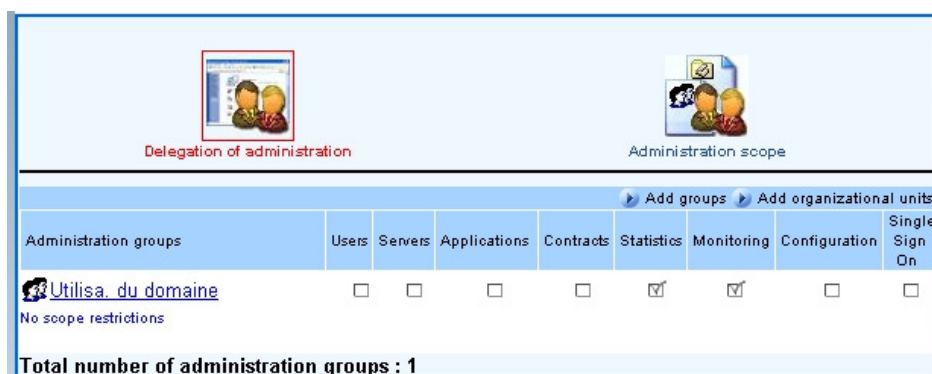


Figure 81 - Administration groups

28.2 Configuring zones

Zones restricting the administration range must be defined before you can assign them to user groups. This will enable you to reduce the visibility of objects to only those elements that are authorized for your delegated administrators.

1. Click on the Configuration menu, then on the Administrators sub-menu.
2. Click on the Administration Zone button.
3. Click on Add a zone.
4. Enter the name of the zone
5. Select the range of the zone (Users, Servers and/or Applications)
6. Click on Next.
7. Select the user groups, then Next.
8. Select the server groups, then Next.
9. Select the application groups, then OK.



Figure 82 - List of zones

28.3 Configuring roles

To configure the Administration roles for a group/OU added as an administration group:

1. Click on the Configuration/Administrators menu.
2. Select an added group/OU.
3. Click on Properties.
4. Check the boxes according to your needs: Users, Servers, Applications, Contracts, Statistics, Monitoring, and Configuration.
5. Click on Next.
6. Select the desired Administration zone
7. Click on OK.

Users

The "Users" role groups together the management of users, i.e. the delegated administrator can add/remove groups or Organizational Units and display the options of the users/groups.

Note: delegated administrators cannot modify the groups of delegated administrators, because they are not visible to delegated administrators in the management of users, for security reasons.

Servers

The "Servers" role allows the management of servers that have already been referenced in AppliDis. It can create or remove server groups. However, only a Domain Administrator can add/remove a server, modify the role of a server or activate or deactivate the virtual IP. Special privileges are required in order to perform these operations.

The administrator can nevertheless display all of this information without modifying them.

The real-time display of the load of the servers can also be found in this administration zone.

Applications

The "Applications" role allows the full management of applications. This includes adding or removing applications or groups of application, modifying existing applications, early referencing (requires local administrator privileges on the targets).

Contracts

The "Contracts" role gives privileges for the whole "Contracts" menu of the administration console. The delegated administrator can display the contracts in progress, add/remove contracts or even modify an existing contract.

Statistics

This allows the AppliDis statistics to be displayed, including a summary of the statistics, display of the statistics by server/application/user and the "Search" entry in the "Statistics" menu.

Monitoring

The "Monitoring" role allows the management and monitoring of the current activity on the AppliDis server farm (information on server loads), of feedback of logs and the option of displaying and interacting with the applications in progress, connected users and associated actions (messages, remote takeover).

Message sending or remote takeover requires special network access privileges; an authentication box will be displayed if the delegated administrator wishes to carry out one of these actions. He will then have to be authenticated as a domain administrator in order to carry out the operation or for any account allowing this operation.

Configuration

The "Configuration" role allows the management of information relating to load balancing and other general functions.

A delegated administrator having privileges to manage the "Configuration" zone will also be able to modify the AppliDis license.

Conversely, he will not have privileges to manage or to display information relating to the AppliDis databases, nor privileges to modify the language of the AppliDis site.

28.4 Removing a group/OU

1. Click on the Configuration/Administrators menu.
2. Select an added group/OU.
3. Click on Remove.

28.5 General remarks about the management of delegated administration privileges module:

The delegated administration roles are cumulative; users that are present in several delegated administration groups will have access to the functions defined for all these groups.

Ensure that the delegated AppliDis administration privileges are consistent with the domain access privileges, as some functions (remote access, addition of servers, activation of alert module) require specific or elevated network access privileges.

The Domain administrators always have all AppliDis administration privileges and these cannot be restricted.

The alarms module can only be accessed by a member of the domain administrators group.

29 AppliDis configuration

This section allows you to enter your license number, parameterize the people who can connect to the AppliDis administration site without being a domain administrator, configure the options of AppliDis users and to save onto the database on which AppliDis is based.

29.1 General information

This page makes it possible to enter your company information, such as name, address, phone number and fax number.

1. Click on Parameters in the main menu. By default, you will be in the General information section.
2. Fill in the various fields and click on OK.

29.2 AppliDis license

By default, the license used on installing AppliDis is a demo license, allowing you to execute applications for 31 days. When your license is about to expire, you will be automatically redirected towards this page. You then have to enter a new license, obtained from your integrator. You can choose from a number of different licenses:

- Demo license limited to a number of fixed executions.
- Standard license which is limited to the installation of a single server and also limits the number of simultaneously connected users (i.e. who have opened AppliDis sessions which have not been closed).
- Advanced license which limits only the number of simultaneously connected users.

Changing licenses

In order to change the AppliDis license, you have to go to the "General Parameters" menu, then in the "License" sub-menu. However, if the demo license has expired, you will be automatically redirected towards this change of license page (all the other pages become inaccessible).

1. Click on Configuration in the main menu. Go to the License sub-menu. (If your license is out-of-date you will be in this page by default)
2. Note the Serial number carefully. You should then contact your integrator, providing this number, in order to get your new license.
3. Your integrator will send you a license in the form of a string of characters.
4. Enter this character string in the Your license field.
5. Click on OK.

29.3 Active Directory

By default, AppliDis Fusion 4.0 selects the domain in which the AppliDis Administration & connection broker servers are located. However, AppliDis manages as well connections from other domains or even from multi-domains.

The user groups can connect to an AppliDis Fusion 4.0 farm from a different domain even if they keep authenticating to the domain they belong to. The main interest is to offer a farm of shared AppliDis Fusion 4.0 virtualized applications for companies which have multiple independent geographical sites.

When a user launches his Microsoft Internet Explorer, the Fusion 4.0 AppliDis web portal displays a domain field. From the drop down list users can select the domain they wish to get connected to.

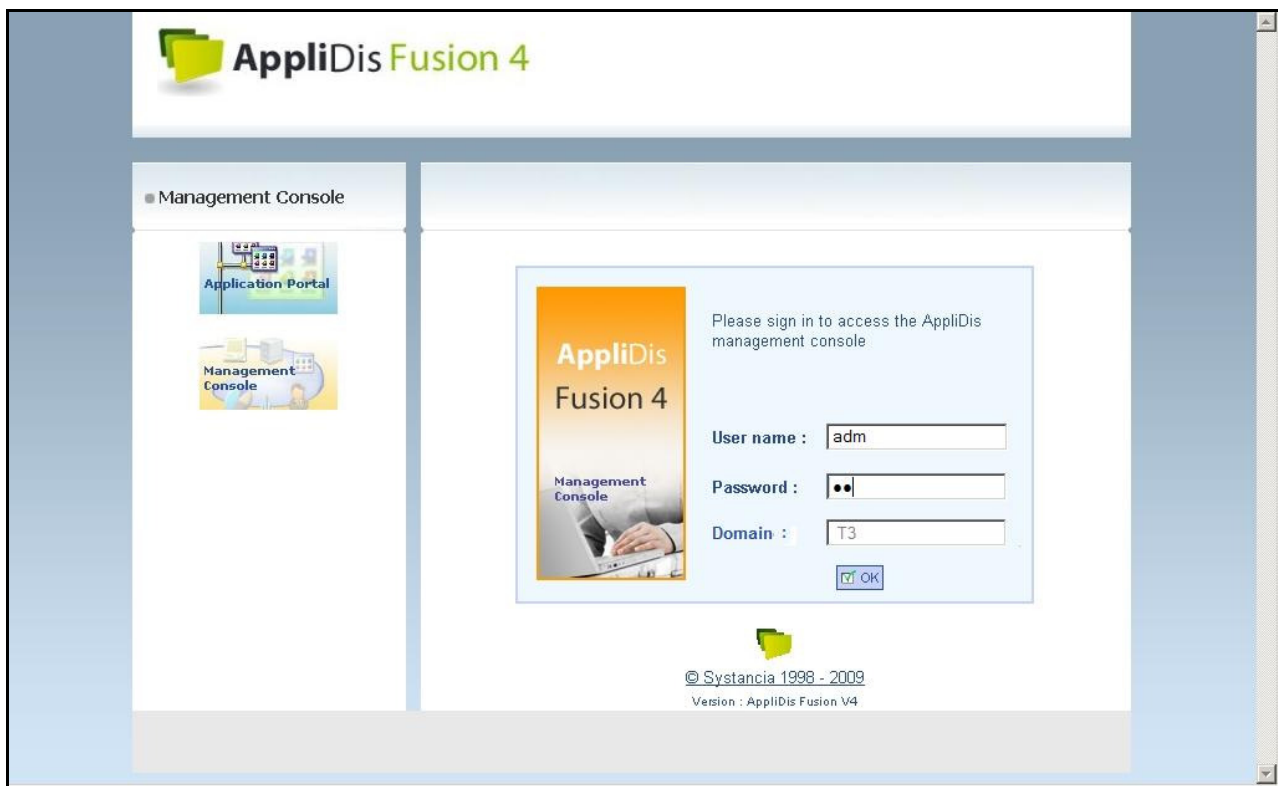


Figure 83 - Multi-domain authentication (AppliDis User Web portal)

All the requests to the Active Directory are established via the user account that connects to the AppliDis web client or to the Administration portal.

AppliDis Fusion 4.0 reads the active Directory information respecting rights of the user account that is part of the Active Directory.

For example, if a delegated administrator wishes to import Active Directory groups within AppliDis Fusion 4.0. If the user does not have access to those Active Directory groups, those groups in question will not be reachable & visible within the AppliDis Administration console.

Functionality Prerequisite

Users from approved domains must be added to the local Active Directory groups which are part of AppliDis Fusion 4.0.

Users must be authorized to get connected to Microsoft Terminal Server on the application hosts servers and Desktop windows.

Moreover, users must be part of the authorized user group which is entitled to get connected to Microsoft TSE.

Functionality Prerequisite

When installing AppliDis Fusion 4.0, the software is configured to import global groups & Organization Units (OUs). Furthermore, it is configured to read the Active Directory which is set with the ADSI mode. In this particular case, AppliDis Fusion 4.0 is linked to the Active Directory from which server AppliDis Fusion 4.0 is installed.

Activation of the multi-domain feature

Please navigate to configuration > Active Directory within the AppliDis Administration console, in order to check the type of available Active Directory. The two options are either ADSI or NetAPI.

Please tick the multi-domain management box in order to activate this feature.

As soon as the local groups are visible within AppliDis Fusion 4.0, they can be imported within AppliDis Fusion 4.0. Several algorithm solutions have been added in order to enhance the local groups search. It allows a greater flexibility & reliability when reading the Active Directory information.

The '**MemberSelection**' algorithm offers the possibility to grab local groups analyzing the **Member** properties of the user, thus discover all the user's local groups with his/her **domain\login** information.

The '**MemberOfSelection**' algorithm offers the possibility to grab local groups analyzing the **MemberOf** properties of the group, thus determine all the user's local groups.

The '**MemberSIDSelection**' algorithm offers the possibility to grab local groups analyzing the **Member** properties of the user depending on his/her unique SID.

The multi-domain management box is grayed out until you click on the top right corner arrow 'update directory connection'.

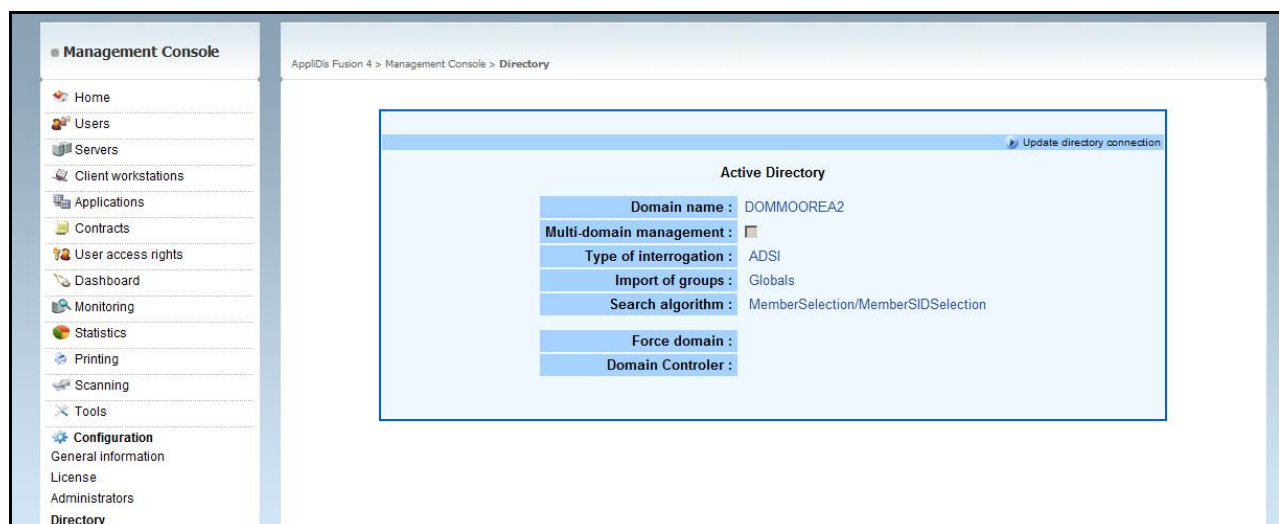


Figure 84 - Active Directory information

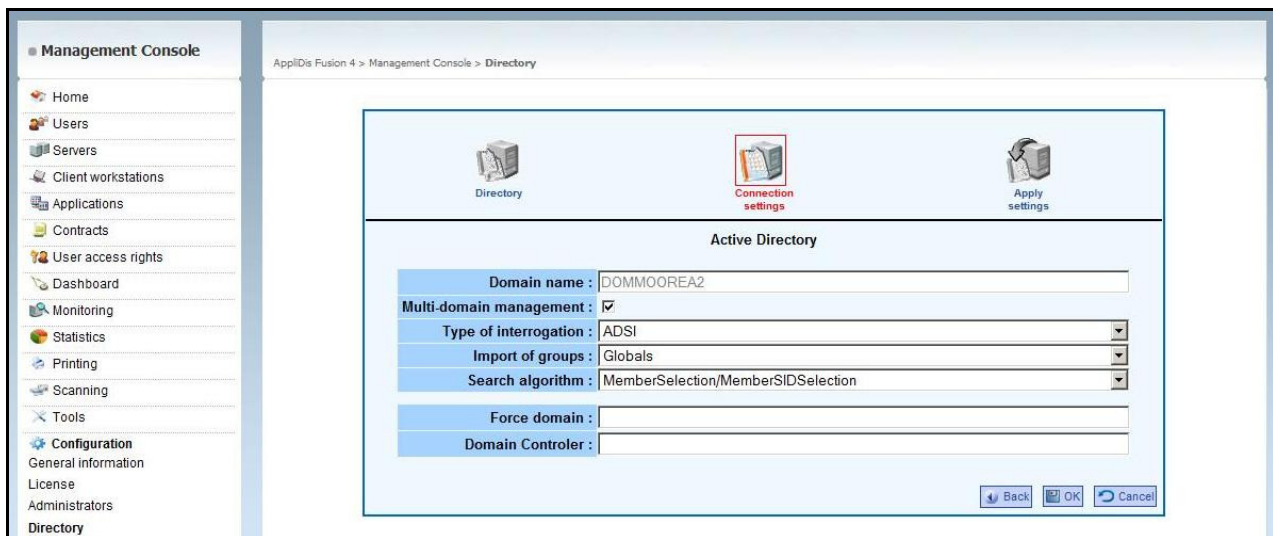


Figure 85 - Active Directory connection settings

1. AppliDis desktop & locked down clients are compatible with the two-way trust* mode.
2. The two-way trust options are available from the AppliDis Administration console (Menu > Configuration > Directory).
3. AppliDis Fusion 4.0 manages local groups which include intra-domain global groups running in NetAPI for the two-way trust mode.

* *One-way trust*: One domain allows access to users on another domain, but the other domain does not allow access to users on the first domain.
Two-way trust: Two domains allows access to users on both domains.

Configuration of the Active Directory options for a bi-directional access

From the AppliDis Administration console (Menu > Configuration > Directory), Administrators have the possibility to modify its configuration (see figure 77 above – Update directory connection). From within the connection settings menu (see figure 78 above), administrators can set & amend parameters.

The following table defines the various available parameters:

Multi-domain management	It activates the multi-domain management feature if the corresponding box is ticked.
Type of interrogation	(Active Directory Service Interface) ADSI or Microsoft Net API
Group imports	It defines the type of group within AppliDis for Microsoft NetAPI or ADSI

Algorithms (search function)	0 : Algo « MemberSelection » for both ADSI & NETAPI modes. 1 : Algo « MemberOfSelection » for both ADSI & NETAPI modes 2 : Algo « MemberSelection » for NETAPI & Algo « MemberOfSelection » for ADSI 3 : Algo « MemberOfSelection » for NETAPI & « Algo MemberSelection » for ADSI 4 : Algo « MemberSelection » for NETAPI & Algo « MemberSIDSelection » for ADSI 5 : Algo « MemberOfSelection » for NETAPI & Algo « MemberSIDSelection » for ADSI By default, the key is set to 4.
Domain Controller	Domain controller name (DC). It allows forcing the Domain controller. You must specify the domain controller with the IP address or the server name.
How to force the domain	It specifies the Netbios name. You must specify the domain name.

29.4 General options

The administrator can configure several options for the AppliDis users. These configurations are then valid for all the AppliDis users executing a new application via AppliDis. The change of option does not affect user sessions that have already been launched, or sessions that were disconnected and resumed after the new configuration.

Application priorities

AppliDis makes it possible to define priorities on applications of "Application priority levels" page 111. The handling of application priority can be activated or deactivated from AppliDis module activations in the options.

1. Click on Configuration in the main menu. Go to the Options sub-menu.
2. In activation of AppliDis modules, check the Scheduling of applications box to activate this option.
3. Click on OK.

Portal and RDP desktop Gateway

Activation of the Gateway module will force all AppliDis clients to use a Gateway Server to connect indirectly to the Application servers. At least one Gateway Server must be installed, either before or after activating this option, in order to be able to use AppliDis.

Dynamic directory binding

AppliDis provides two methods to manage users:

- **Synchronized management** (check box deactivated): AppliDis users must be imported by the Administrator then synchronized with your directory. This synchronization operation must moreover be carried out at each modification of groups in your Directory (Active

Directory, Novell, OpenLDAP, etc.). This mode is recommended for slow or not very powerful directories.

- **Dynamic management** (check box activated): Users are not imported into the database. Users are added to the groups selected in AppliDis each time the user connects to the portal. Thus, any modification made in your Directory (Activates Directory, Novell, OpenLDAP, etc.) takes immediate effect on AppliDis without any intervention required by the AppliDis Administrator.

Automatically save applications

When this option is activated (default setting), the applications detected by AppliDis are automatically referenced in the list of applications. You can deactivate this option and thus stop this mechanism at any time. The automatic referencing task consists in adding applications to AppliDis and automatically creating the associated icons.

Link between workstations and server Groups

This option allows management of client workstations to be activated according to their IP address ranges, in order to connect them to a server farm.

Link between workstations and server Groups

This feature allows to choose the publication mode of an application or of a desktop depending on users' needs for clients (Web portal, Desktop and locked down desktop).

Administrators can determine a different access to the applications and to the desktops depending on the publication mode selected. Hence, administrators can give access to your applications & to your desktops depending on your connection location (within the company or remotely) authorizing or denying access to one of the access modes (Web portal, Desktop and locked down desktop).

MyApps Catalogue

This feature allows Administrators to manage the 'MyApps AppliDis applications catalogue'. When this option is ticked, a new menu « MyApps catalogue » is displayed within the AppliDis Administration Management console.

Automatic connection

Users must be authenticated by means of their domain login and password in order to be able to access their application portal or to be able to execute applications from AppliDis Desktop.

If automatic connection is activated, AppliDis checks that the person who is trying to access the AppliDis site or launch an application from AppliDis Desktop is properly identified and connected to the network by the domain controller. If this condition is verified, AppliDis allows access to the AppliDis client site or allows the application to be launched by AppliDis Desktop without requesting a password.

This access is based on AppliDis keeping the user's password in an encrypted form. If the option is checked, the user's password is preserved in an encrypted form provided that the user accepts automatic connection.

"Smart Connection" technology

The user is offered two reconnection options which will allow him to continue his work, either in the event of a network disconnection, to automatically resume a job that was previously opened from another workstation, or to continue working on an application while making nomad connections from several workstations, automatically and without disconnections.

- **Automatic resumption of disconnected applications:** upon making a new connection, any disconnected applications are automatically proposed to the user.
- **Automatic resumption of open applications:** upon making a new connection, any applications opened on another workstation will be proposed to the user.

Activate local files and folder access optimization

This option allows activating (box ticked) the optimization access to local files and folders from the AppliDis application servers.

Activate VDI service

Activate desktop anticipation

This option relies on the AppliDis Fusion 4.0 load balancing engine which is used to start or get out of 'stand by' mode of virtualized client machines before it is requested by the users. This feature aims at anticipating a client machine to request an application/a session to be launched based on the historical data of the load balancing engine. Hence, users do not need to wait for the client device to start or get out of the 'stand by' mode. Access time to the machine and entering user login are the only steps needed before having access to the applications.

Activate TS/RDP desktops

When this box is ticked and one AppliDis application server is available within AppliDis Fusion 4.0, a desktop is automatically displayed within the list of desktops. It is called « RDPDesk ».

It offers users to have access to a full desktop which will be launched by an AppliDis application server. It does correspond to the Operating system on which it is launched (Microsoft Windows 2000, 2003 or 2008).

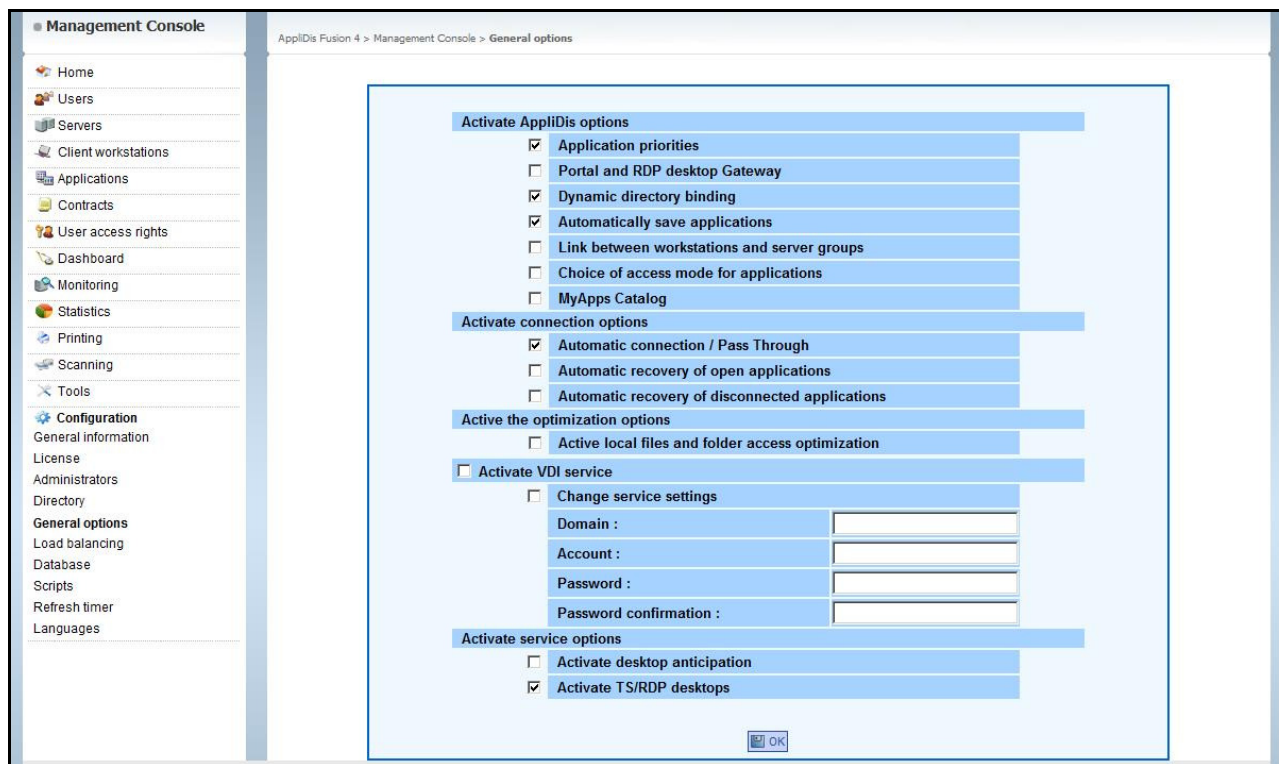


Figure 86 - Configuration of AppliDis general options

29.5 Load balancing

Load balancing between different AppliDis servers hinges on 4 criteria:

- **Static characteristics of the Application servers:** These gather the characteristics of the server in question, for example the amount of RAM, the power of the processor, etc.
- **Dynamic characteristics of the Application servers:** These correspond to the amount of random access memory available, the processor occupancy rate at the time of the connection request, etc.
- **User behaviour based on application and servers (learning matrix):** This element is based on learning and predicting user behaviour. For example, every Friday a user uses the planning application, which is only present on one of the servers. If this user launches another application which is present on 2 servers, one of which is the one that has the planning application, AppliDis will prefer to open the application on this server, anticipating the fact that the user will launch the planning application later on.
- **Behaviour of intra-server sessions in training:** This criterion tends to distribute an equivalent number of sessions on each server (Warning: several applications operating in APPLICATION mode on a given server share the same session on this device).

You can decide to give more or less importance to each of these parameters from the load balancing configuration page.

The option "**Give priority to the user's open sessions**" will modify the behaviour of the load balancer when an application is started. Indeed, if the user is already executing an application via AppliDis, any new application started by this user will be executed in the same session. The required conditions are for the application to be present on the server and acceptable availability in terms of resources.

The values set when AppliDis is installed allow rational load balancing and provide a natural distribution between the different servers.

Furthermore, please note that a system to protect against the "Black-Hole" effect is in place in the AppliDis load balancing engine. This makes it possible to artificially lower the grade of a server receiving a certain number of simultaneous connections. What may happen is that when the system is under load and a new unit is added, the new unit may be repeatedly selected by the load balancer, taking into account the imbalance of the calculated load. The server grade that is lowered in this way is valid until the server information is updated. Terminal Servers do not in actual fact readily support very fast session opening requests.

Adjusting parameters

1. Click on Configuration in the main menu. Go to the Load balancing sub-menu.
2. Click on the left arrow to lower the importance of a parameter. Click on the right arrow to increase the importance of a parameter.
3. The bar chart on the right directly displays the importance of one parameter compared to the others.
4. When you are satisfied with the distribution of importance between your various parameters, click on OK.

Default settings

1. Click on Configuration in the main menu. Go to the Load balancing sub-menu.
2. Click on the Default values button to find the default settings.
3. A message will ask you to confirm your choice; select OK.

Multimedia

With application servers running Windows 2008 R2, your users will have access to full multimedia features such as video, two-way sound, Flash and Silverlight.

These functions can be activated from a server's properties (provided the server is running Microsoft Windows Server 2008 R2).

You are able to configure the following settings:

- Multi-monitor mode,
- Remote audio player,
- Remote audio recording,
- Multimedia flows.

Secondary databases

Secondary databases are managed directly from the AppliDis Administration console from the Configuration / Databases menu. This administration page can be used to consult the configuration of your databases, add or remove secondary databases and switch between databases.

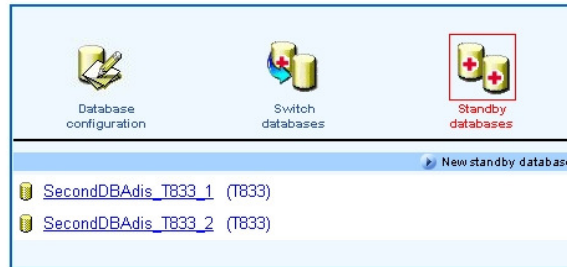


Figure 87 - Configuration of backup databases on the AppliDis Administration console

29.6 Creation of backup databases

Secondary databases must be created in order to ensure the high availability of data. You must choose between SQL 2000, SQL 2005 or SQL 2008. This is regardless of the main database type defined on installing the CD ROM. Up to 5 secondary databases can be added.

Microsoft SQL Server secondary database

The following parameter settings are required in order to deploy an SQL Server backup database:

1. On the Configuration/Database page, click on Backup database.
2. Select SQL Server 2000 database type.
3. Fill in the name of the SQL server hosting the database in the Server field followed, if necessary, by "\ NOM_INSTANCE" (\ NAME_INSTANCE), or select the database from the drop-down list.
4. Fill in the path to the database of the database server.
5. Fill in the name of the database
6. Fill in the account for access to the database and its password.

Note: The SQL account must have System Administrator privileges on the database.

Figure 88 - Creation of an SQL backup database on the AppliDis Administration console

SQL 2005/2008 standard/Express secondary database

The following parameter settings are required in order to deploy an SQL Server backup database:

1. On the Configuration/Database page, click on Backup database.
2. Select SQL EXPRESS database type.
3. Fill in the name of the SQL server hosting the database in the Server field followed, if necessary, by "\ NOM_INSTANCE" (\ NAME_INSTANCE), or select the database from the drop-down list.
4. Fill in the path to the database of the database server.
5. Fill in the name of the database
6. Fill in the account for access to the database and its password.

Figure 89 - Creation of a backup database using the internal engine (AppliDis Administration console)

29.7 Scripts

AppliDis enables you to start a sequence of scripts or executables when a session is opened on a given server. These scripts can be parameterized by server. You will thus be able to launch commands or executables which will be started before your published applications. A command script for example will carry out operations regarding the assembly of network drives. While parameterizing an executable at the start of a session, you will be able to launch "demon" type programs which turn your users' sessions into background tasks.

The scripts started can be either synchronous or asynchronous. In synchronous mode, AppliDis will wait for the end of the script in order to continue the sequence (the script should not be blocking). In asynchronous mode, after the start of the process, AppliDis will call up the following sequence directly, without waiting for the end of the script or process.

Scripts are only started when a new session is opened.

Setting the parameters of a new script

1. Click on Configuration in the main menu. Go to the Scripts sub-menu.
2. Select the server on which to execute scripts using the drop-down menu. If some elements are already present in the list, the new script will be inserted at the end of the sequence.
3. Click on the New Script button
4. Enter the command line for your script. You can use the Browse button to help.
5. Check the "Await end of script" box if your script must be synchronous.
6. Click on OK.

Modifying the sequence of execution of scripts

1. Click on Configuration in the main menu. Go to the Scripts sub-menu.
2. Select the server on which you wish to modify the sequence of scripts.
3. Use the "Up"/"Down" buttons to move a script in the sequence of execution.
4. Click on OK to save the modifications.

29.8 Languages

The language in which AppliDis will be executed can be changed. These modifications will affect all AppliDis interfaces, particularly the administration console, the user portal and the AppliDis Desktop module. The range of this parameter setting concerns all the clients connected to your Administration Server.

Modifying the language display of AppliDis

1. Click on Languages in the main menu.
2. Select the desired language.
3. Click on the "Apply" button.



30 Database maintenance

30.1 Requirements

It is essential to have a successful database backup before using this feature. The database maintenance must be carried out out of hours when no users are connected to the system.

30.2 Manual data cleansing

30.2.1 Resetting data usage statistics

This option can be used to remove all statistics data related to current and historical user connections. Any sessions left showing in the dashboard disappear, however, the AppliDis sessions are not reset.

30.2.2 Reset data usage statistics and imported users

Same as above with all imported user accounts removed from the AppliDis database.

30.2.3 Reset data usage statistics, imported users and created contracts.

Includes the points 1 and 2 as well as the removal of all the AppliDis contracts created (No applications will then be available).

30.2.4 Reset data usage statistics, imported users, created contracts and imported user groups.

Includes the points 1, 2 and 3 as well as the removal of all imported user groups. Subsequently new user groups will have to be imported and new contracts created.

30.2.5 Reset created contracts and user access tokens in use.

This option resets the table contract to its original state by default. If you remove all the statistics with users connected and the user access tokens in use are not updated. This alternative resolves this issue. Tokens can then be unsynchronised if a database is brought back in the middle of a live environment (This method is not recommended).

30.3 Automated data cleaning

The data cleansing can be automated. The data cleansing can be set to run automatically at regular interval.

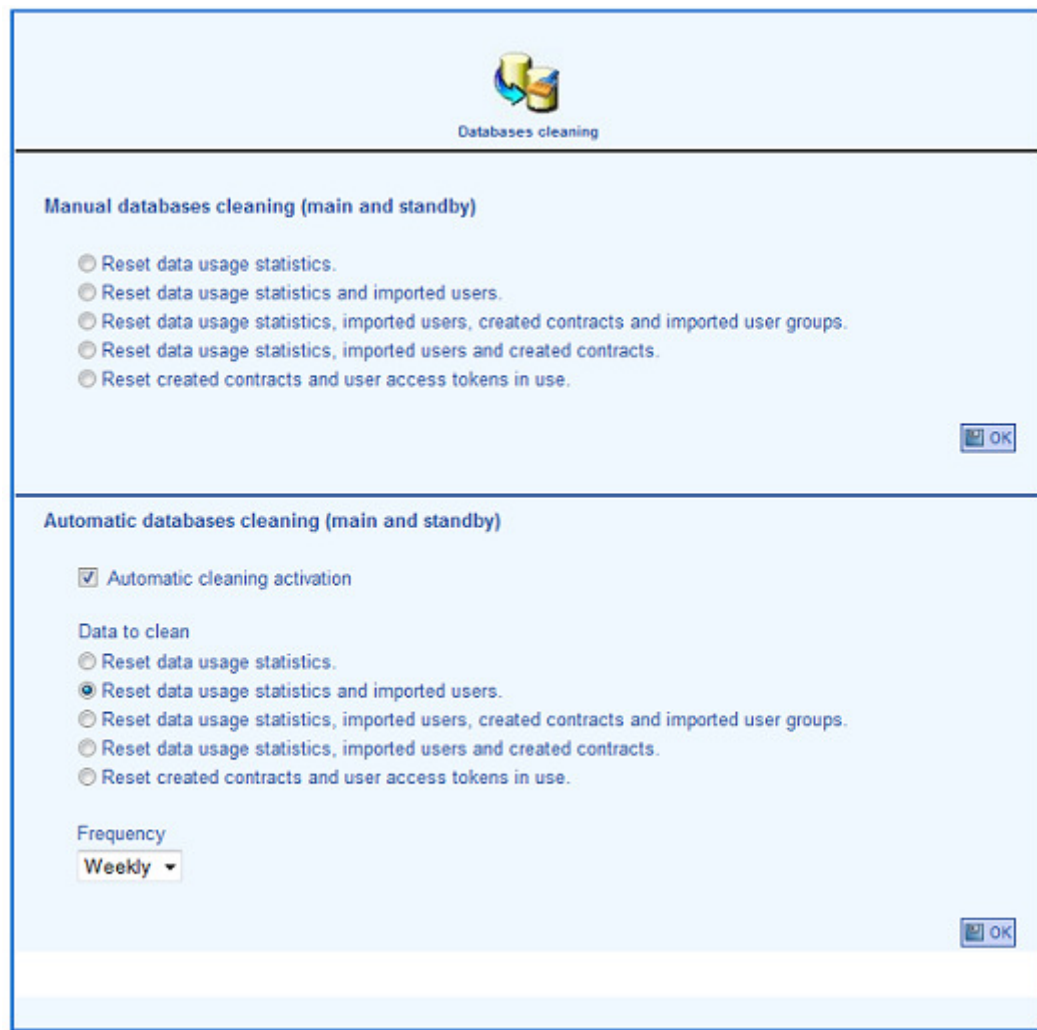


Figure 90 – Database cleansing menu

30.4 Restoring the main database

In the event of an issue on the main database, AppliDis switches automatically to safe mode.

To control the state of the database:

1. From the menu Configuration/Database, click on Database configuration.
2. If the message ALARM: APPLIDIS DATABASE RUNNING IN SAFE MODE is displayed, then AppliDis is relaying on the standby database.



Figure 91 – Notification database in safe mode

The AppliDis administrator has to connect to the administration console to switch back to the main database. This must be done in one of two ways, as chosen by the Administrator, after the database has been restored.

Connecting to the main database without updating of the information stored in the standby databases.

1. On the Maintenance/Switch Database page.
2. Select Switch to the main database without transfer from the standby database.
3. Click on OK.

Connecting to the main database with updating of the information stored in the standby database to the main database

1. On the Maintenance/Switch Database page.
2. Select Update the main database from the standby database and make it live.
3. Click on OK.

Note: It is recommended to connect a new database outside of production hours.

When connecting directly to the main database after an incident, the backup databases can be updated simply by removing and then recreating them; this should also be done outside of production hours.

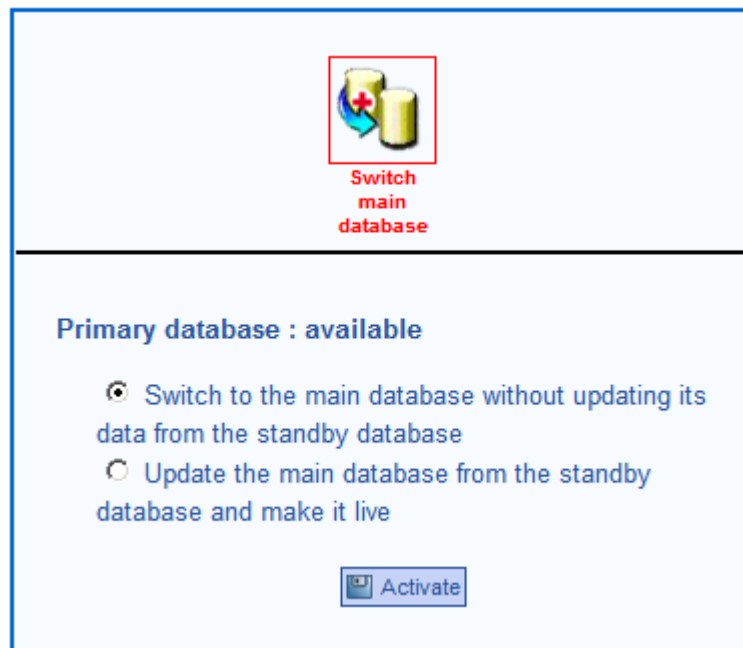


Figure 92 – Switching back to the main database

31 Advanced configuration and operation of AppliDis Fusion

This chapter describes the various AppliDis configuration and maintenance operations.

1 AppliDis ToolBox

Via the administration console, the administrator has access to a "Tools" function providing access to advanced configuration tools. These tools are a mix of command-line and Windows GUI utilities which enable advanced modifications for configuration or maintenance. They are classified by category, and each component is described. Specific instructions for use are usually available.

2 Saving information (Backup)

The technical information regarding AppliDis parameter settings are all located in the AppliDis databases. This information must therefore be saved regularly. From a save of the AppliDis database, you can redeploy your whole system by means of the "**setup**" feature and then recover all your parameter settings as they were. Your applications must however be installed as parameterized in the database at the time of the save.

2.1 Backing up databases

Database saves should preferably be made when no users are working, to guarantee the consistency of the statistics. The following methods of saving are provided by way of example; any other tried and tested method of saving data will also be suitable. Ensure that the procedure does not interfere with other applications, particularly when you stop IIS, since this could cause an interruption of service if a website is published on the AppliDis administration server.

Saving an SQL database from Enterprise Manager

If your database is of the SQL Server type (MSDE, 2000, 2005, 2008 or 2005/2008 Express) and you have the Microsoft Enterprise Manager tools, proceed as follows to save the database. Knowledge of the Microsoft Enterprise Manager tools is necessary.

1. Connect to the database server using the Enterprise Manager tools.
2. It is recommended that no user should be working with AppliDis.
3. Select the database (For example, the name provided at installation).
4. In the "All tasks..." menu, select Save.
5. Specify a full save.
6. Specify the destination directory and the file name for the backup.
7. Save the file in a secure place.

Manually saving an SQL database

If you do not have the Microsoft Enterprise Manager tools, the following method can be used to save an AppliDis database operating under MSDE for example. However, Systancia recommends the use of the Microsoft Enterprise Manager tools for these operations.

1. Locate the SQL database server.
2. Locate the name of the AppliDis database (specified at the time of installation).
3. Locate the site of the MSDE database instance which is, by default, as follows:
c:\Program Files\Microsoft SQL Server \ MSSQL.1 \ MSSQL \ Data \
4. Ask all your users to disconnect (stop production).
5. Stop IIS services (World Wide Web publication Services) on all AppliDis Administration servers.
6. Stop the SQL Server service on your database server.
7. In the folder corresponding to database instance, copy the files: SqlApplidisBase_Data.MDF and SqlApplidisBase_Log.LDF where SqlApplidisBase is the name of the default AppliDis database.
8. Start the SQL Server service.
9. Start the IIS services on all Administration servers.

2.2 Restoring databases

The restoration of the database should be carried out when no user is working on the platform, to guarantee consistency of the statistics.

Restoring an SQL database from Enterprise Manager

If your database is of the SQL Server type (MSDE, 2000, 2005, 2008 or 2005/2008 Express) and you have the Microsoft Enterprise Manager tools, proceed as follows to restore the database. Knowledge of the Microsoft Enterprise Manager tools is necessary.

1. Connect to the database server using the Enterprise Manager tools.
2. It is recommended that no user should be working with AppliDis (stop production).
3. Save your data.
4. Stop IIS on all the AppliDis Administration servers.
5. Select the database (For example, the name provided at installation).
6. In the "All tasks..." menu, select Restore.
7. Specify the source directory and the file containing the save and restore.
8. Start IIS on all the Application servers.

Manually restoring an SQL database

If you do not have the Microsoft Enterprise Manager tools, the following method can be used to restore an AppliDis database operating under MSDE for example. However, Systancia recommends the use of the Microsoft Enterprise Manager tools for these operations.

1. Locate the SQL database server.
2. Locate the name of the AppliDis database (specified at the time of installation).
3. Locate the site of the MSDE database instance which is, by default, as follows:
c:\Program Files\Microsoft SQL Server \ MSSQL.1 \ MSSQL \ Data \
4. Stop IIS services (World Wide Web publication Services) on all AppliDis Administration servers.
5. Stop the SQL Server service on your database server.
6. In the folder corresponding to database instance, copy the files: SqlApplidisBase_Data.MDF and SqlApplidisBase_Log.LDF where SqlApplidisBase is the name of the default AppliDis database, then replace them with your backup files.
7. Start the SQL Server service.
8. Start IIS on all the Application servers.

2.3 Backing up files

Backing up files is not compulsory, and relates to the icons displayed to users. These will be automatically repopulated by AppliDis progressively if the option "**Automatic saving of Applications**" is active (default configuration, see page: 185). These files can be saved at any time, on all Administration servers :

1. Locate the AppliDis installation path, by default:
C:\Program Files\Systancia\AppliDis
2. Save the DisFiles sub-directory
3. Save the Web\Application icons sub-directory

2.4 Restoring files

The icon resource files must be located as follows:

1. Locate the AppliDis installation path, by default:
C:\Program Files\Systancia\AppliDis
2. Restore the DisFiles sub-directory
3. Restore the Web\Application icons sub-directory

2.5 Saving registry keys

Some configuration information is stored in registries, in a redundant way with the configuration of the database.

These keys will be positioned automatically when an Administration Server is connected or when deploying a Gateway or Application Server.

1. Save the key and sub-keys HKLM\SOFTWARE\Systancia\
2. Save the key and sub-keys HKLM\SOFTWARE\Infostance\

3 Database management

AppliDis databases are intended to provide continuity of service in case of a disruption. The information contained in the backup databases and the main database is identical in nature. If the main database goes down, an alert is raised and AppliDis switches to backup mode. The main database is reconnected in a variety of ways, (see

, p. 191), with the transferral of data from the backup database to the main database (synchronisation), or without data transferral.

3.1 Resetting the data of the backup databases

To reset the data in a backup database, it must be deleted and then recreated. These operations should be carried out outside production hours when no users are connected.

3.2 Restarting a database server

It is recommended not to stop the AppliDis database servers. If you have to do this for maintenance purposes, follow the security procedure below, outside production hours:

1. Stop IIS services (W3SVC) on the administration servers which do not have the virtual IP.
2. Stop IIS services (W3SVC) on the Administration Server with the virtual IP.
3. Carry out your maintenance operations.
4. Start IIS services (W3SVC) on the Administration server which had the virtual IP.
5. Start IIS services (W3SVC) on the other Administration servers .

Note: Distinguishing between the Administration Server with the virtual IP and the other servers is only useful if you distinguish between main Administration servers (with the virtual IP) and the others. It is not important for operation of AppliDis.

4 Restarting the servers

4.1 Restarting an Administration server

In redundancy mode with virtual IP protection, it may happen that a server breaks down or stops:

1. Connect to the Administration console by using the URL of an Administration Server which will not start.
2. In the Servers/Virtual IP menu, force the virtual IP on the server where you are connected.
3. When the virtual IP is set to the server which will not restart, you can stop the other server.

4.2 Sequence for restarting a server which is both Admin and SQL at the same time

If your SQL databases are installed on two Administration servers in redundant configuration, stop your servers and start them again in the following order:

1. Stop the server hosting the secondary database.
2. Stop the server hosting the primary database.
3. Carry out your maintenance operations.
4. Start the server hosting the primary database.
5. Start the server hosting the secondary database.

If you wish to program a restart of all your servers (by the task planner, for example), it is difficult to program a restart after a stop of a few minutes. Proceed by script to the following sequence (each operation being 5 minutes apart, for example):

1. Stop IIS services (W3SVC) on the server hosting the secondary database.
2. Restart the server hosting the primary database.
3. Restart the server hosting the secondary database.

4.3 Restarting an Application server

There is no contraindication on restarting an Application server, apart from some possible inconvenience for connected users. We recommend the following procedure:

1. Exclude access by new users on this server by stopping the "AppliDis Application Server" service with either of the following methods:
 - a. By deactivating the server from the Dashboard on the Administration console.
 - b. By script on the application server: `NET STOP ADISERVER`
2. Give your users time to close their jobs and wait until they leave the server. In the list of applications on the Dashboard, the server filter allows you to display only the applications in service on a given device.
3. You can stop the server as soon as all work has been stopped.

This procedure is applicable during production hours. However, attention should be paid to the additional workload generated on the other servers in production.

5 Maintenance of AppliDis servers

5.1 Replacing an Application server

Restoring a backup

AppliDis does not put any constraints regarding restoration of a server. If your backup is old however, we recommend removing and adding the "application server" or "gateway server" role from the AppliDis servers menu. This will ensure that the latest version of the module is executed on this server (in case patches or hot fixes were integrated on the backup).

Ensure however that the Microsoft machine account is valid, otherwise system malfunctions are possible. In case of doubt, switch your server onto Workgroups, reset the machine account in your AD, regenerate the server SID if necessary, and then reintegrate your server in the domain.

Rebuilding a server

If you want to reassemble your server with the same features, then after installing all your applications in the same place, proceed as follows in the AppliDis Administration console:

1. Select this server (the Application server check box will be activated).
2. Click on "Modify role".
3. In this list, the Application server check box will be deactivated!
4. Check the box then click on "Apply".

If your applications are installed on different sites, you can modify them manually later on.

5.2 Changing the IP address of an Application server

If you change the IP address of an Application server, you must fill in the new application server IP address in this server's properties, from the administration console. Otherwise, this server may be seen by AppliDis as inoperative (See card IS00156).

5.3 Renaming an Application server

If you have direct access to the database

Carry out the procedure below to rename an Application server (not Administration server). To do this you must have direct access to the database tables and know how to use SQL Enterprise Manager.

1. From the AppliDis administration console, remove the "application server" role and possibly also the "gateway server" role using the "Modify role" menu. Do not remove the server!
2. Rename your server using the appropriate Microsoft procedures (workstation properties).
3. Restart the server that has just been renamed.
4. In the main database, modify the MACHINES.NOM file (replacing the old name with the new one).
5. Repeat these operations for any backup databases you may have.
6. Restart IIS service (Publication of World Wide Web services or W3SVC) on all your Administration servers.
7. From the AppliDis administration console, add the "application server" role and possibly also the "gateway server" role.

If you do not have direct access to the database

To rename an Application server (not Administration server) in the AppliDis advanced version only, proceed as follows:

1. From the AppliDis administration console, remove the "application server" role and possibly also the "gateway server" role using the "Modify role" menu. Do not remove the server!
2. Rename your server using the appropriate Microsoft procedures (workstation properties).
3. Restart the server that has just been renamed.
4. From the AppliDis administration console, go to the servers menu.
5. Add the new server (automatic or manual addition).
6. Apply advanced referencing with the old server as source and the new server as target (the parameter settings of the applications will be transferred).
7. Manually adjust any access privileges that you have set for this server.
8. Test the access to your server by launching an application for example.
9. In the list of the servers, you can remove the server bearing the old name.

5.4 Renaming an Administration server

Renaming an Administration server involves uninstalling it. After uninstalling, the Administration Server role is automatically removed. Rename the device then reinstall AppliDis. Caution: this operation is not possible if your Administration server is a domain controller.

6 Applications Isolées

Présentation de l'isolation système

Principe

L'isolation système consiste à installer une application sur des machines virtuelles cliente (XP/Vista/Seven), à référencer ces machines en tant que serveur d'applications dans AppliDis et à publier l'application dans AppliDis.

Les systèmes client XP/Vista/Seven étant limités à l'ouverture d'une seule session, un seul utilisateur à la fois peut utiliser les applications installées sur ces machines.

Il est par contre nécessaire d'avoir autant de machines virtuelles que d'utilisateurs simultanés autorisés à accéder à l'application isolée.

Intérêt

Ce mode de fonctionnement permet d'éviter les soucis que peuvent rencontrer certaines applications dans un environnement multiutilisateurs. La limite d'une seule ouverture de session sur les machines virtuelles isolées garantit qu'un seul utilisateur à la fois utilisera l'application sur une machine donnée.

L'isolation système permet également d'offrir un environnement système client complet XP/Vista/Seven. Ceci permet également de virtualiser des applications qu'il n'est pas possible d'exécuter sur un système serveur.

Référencement d'une application isolée dans AppliDis

Pré-requis

Les pré-requis à appliquer sur la machine virtuelle client XP/Vista/Seven sont détaillés dans la fiche AppliDis IS00239 – Pré-requis VDI.

Référencement d'une machine virtuelle client

Ouvrez une console d'administration AppliDis, allez dans le menu « Liste des Serveurs » et cliquez sur le bouton « Ajout manuel de serveur ».

Tous

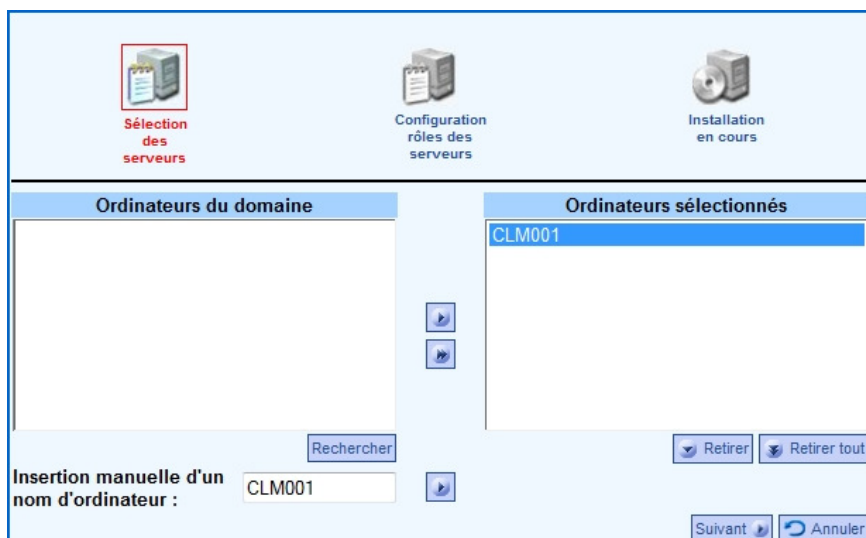
Groupe

DEFAULT

		Ajout hôte machines virtuelles	Ajout manuel serveurs	Ajout automatique serveurs		
Nom du serveur	Rôles :	Administration et connexion broker	Portail web utilisateurs	Gateway	Hôte applications et bureaux	Hôte machines virtuelles
T948		☒	☒	☐	☒	☐
Total de 1 serveur d'infrastructure						
T948		☒	☒	☐	☒	☐
Total de 1 hôte applications et bureaux						

Figure 93 - Liste des serveurs AppliDis

Sélectionnez la machine virtuelle client XP/Vista/Seven à utiliser en tant que serveur d'applications et cliquez sur le bouton « Suivant ».



Sélection des serveurs

Configuration rôles des serveurs

Installation en cours

Ordinateurs du domaine

Ordinateurs sélectionnés

Figure 94 - Choix de la machine d'isolation

Cochez la case « Serveur hôte applications et bureaux » et cliquez sur le bouton « Installer »

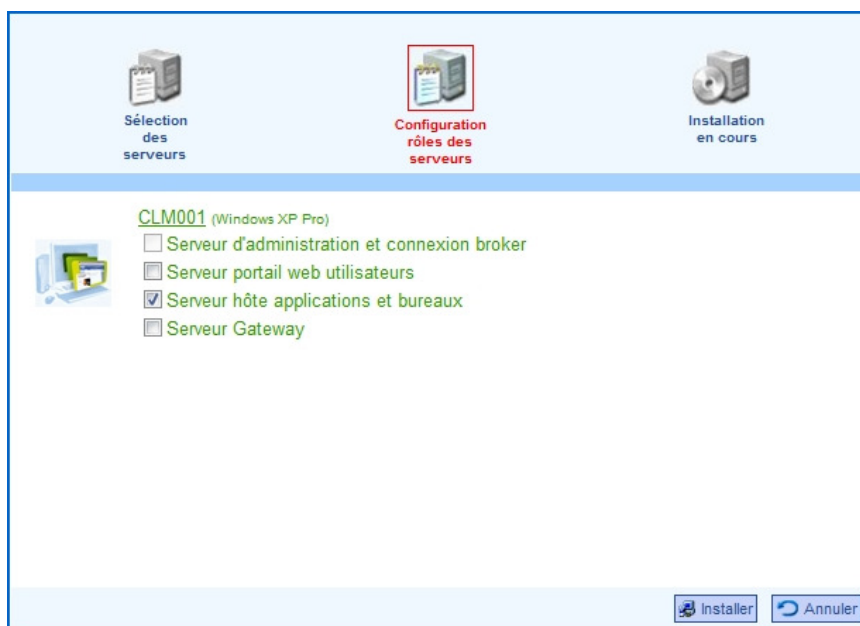


Figure 95 - Installation du rôle serveur d'applications sur la machine virtuelle

Une fois le rôle installée, cliquez sur le bouton « Retour ».

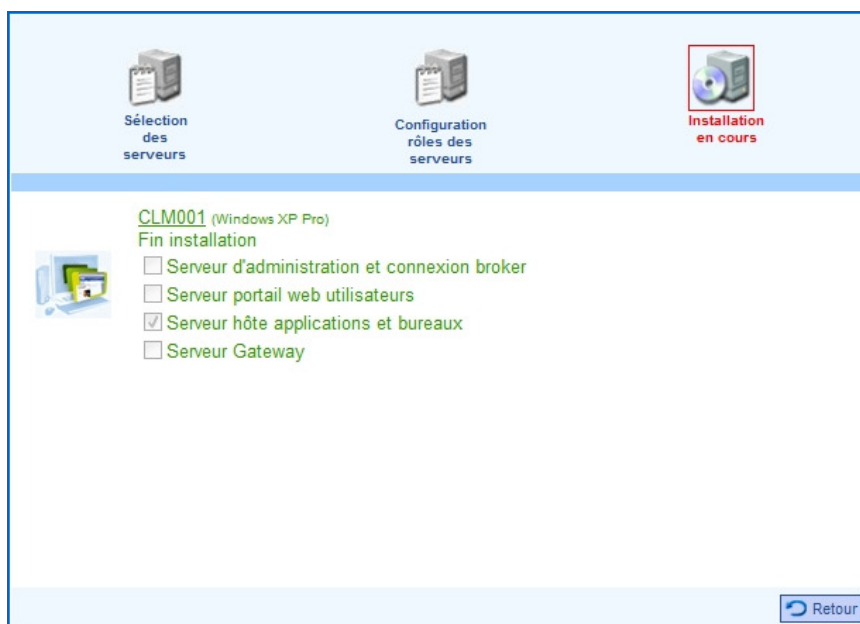


Figure 96 - Fin de l'installation du rôle serveur d'applications

La machine isolée apparaît désormais dans la liste des serveurs en tant que serveur d'applications.

Nom du serveur	Rôles :	Administration et connexion broker	Portail web utilisateurs	Gateway	Hôte applications et bureaux	Hôte machines virtuelles
T948		☒	☒	☐	☒	☐
Total de 1 serveur d'infrastructure						
CLM001		☐	☐	☐	☒	☐
T948		☒	☒	☐	☒	☐
Total de 2 hôtes applications et bureaux						

Figure 97 - La machine isolée est un serveur d'applications

Référencement d'une application sur un système isolé

Le référencement d'applications sur une machine isolée s'effectue de la même manière que sur un serveur TS.

Création d'un contrat sur une application isolée

La création de contrat entre un groupe d'utilisateurs et une application isolée s'effectue de la même manière que pour une application référencée sur un serveur TS.

7 AppliDis VDI

7.1 AppliDis VDI service rights

From the [AppliDis administration server](#), open the services manager snap-in interface (*Start → Run → services.msc*) and display the properties of the [AppliDisVDIService](#) service.

From the *Log On* tab, make sure the service runs under a domain administrators' account. Select the radio button: *This account* and type the account name or browse the directory, and enter the password of a domain administrator.

A domain administrator account is necessary for the automation of any desktop creation. Files are transmitted between the AppliDis administration server and the referenced virtual machine via WMI.

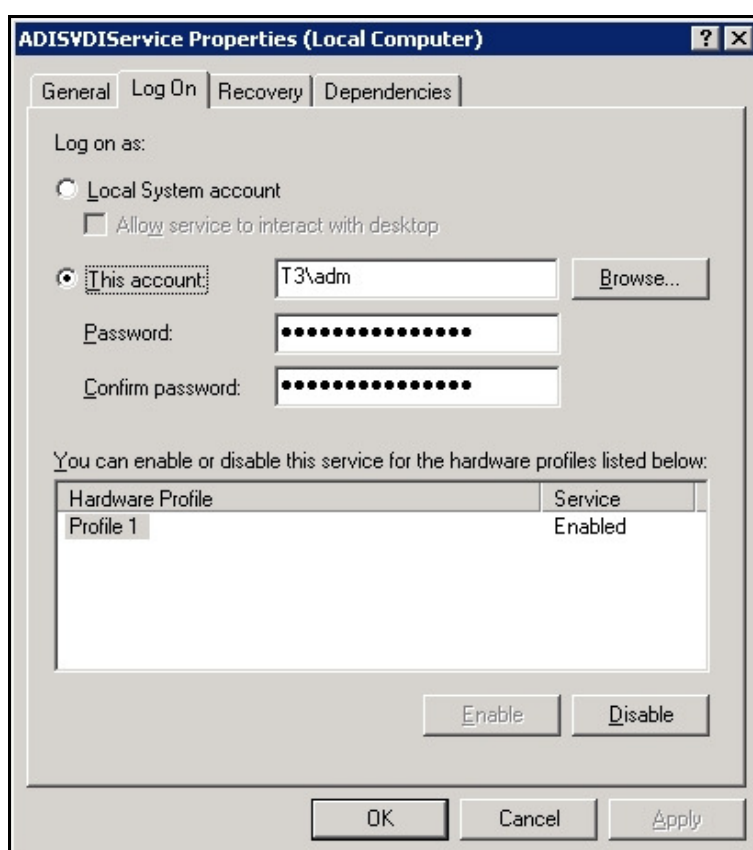


Figure 98 - ADISVDSIService Properties (Local Computer)

7.2 Microsoft Internet Explorer certificate validity

From the AppliDis Administration server, open Microsoft Internet Explorer and go to the browser options (*Tools → Internet Options → Advanced*). Then uncheck the 3 checkboxes below:

- Check for publisher's certificate revocation
- Check for server certificate revocation (requires restart)
- Check for signatures on downloaded programs

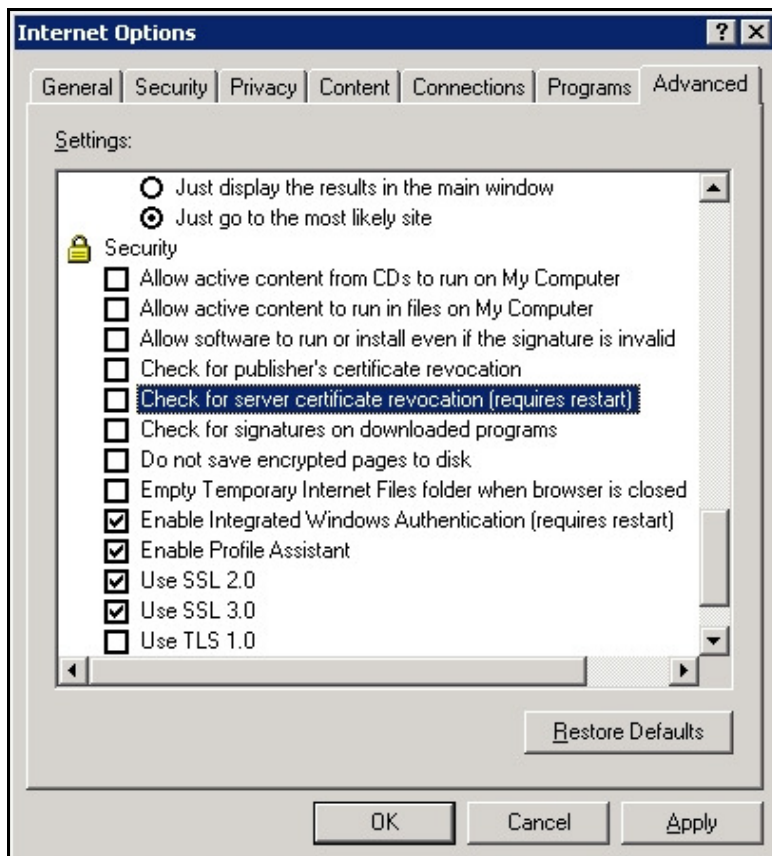


Figure 99 - Security (Internet Options)

Configuration of a virtual machine

7.3 Creation of a virtual machine reference

AppliDis VDI requires the creation of a virtual machine that will serve as a master reference for all subsequent desktops.

Desktops creation via AppliDis VDI is made by cloning the virtual machine called 'reference'. In this way, each new desktop has the same configuration as the referenced machine.

This virtual machine has the following prerequisites:

- It must be created, available and bootable from VMware Virtual Center (no template).
- An installed and functional Microsoft 32bit operating system (Windows XP; Windows Vista or Windows Seven).
- The machine must be a member of the domain.

7.4 Configuration of a virtual machine reference

To automate the creation of desktops, a virtual machine master reference must be configured as follows:

1. The Microsoft Windows **firewall** must be disabled.
2. User groups connecting to the machine must be allowed **remote desktop access**.
3. The reference machine must allow reads and writes to the **remote registry**.
4. The reference machine must allow **remote procedure calls (RPC)**.
5. The reference machine must allow **WMI requests** called by domain administrator & **COM+ events** management.
6. **VMWare Tools** must be installed and up to date on the referenced machine.
7. **Applications** available to the user on his/her desktop must be installed and configured on the referenced virtual machine.

The newly created desktops are cloned from this reference machine, and duplicate all its settings and applications.

The details of this configuration are described later in this document.

Note: The following actions must be performed on a client virtual machine. This machine will be used to create users virtual desktops. This machine will not be directly available to users, but will serve as a master with all subsequent machines being clones of the master.

1. **Disable Microsoft Windows firewall**

In *Start → Control Panel → Windows Firewall* menu, select Off option in the General tab.

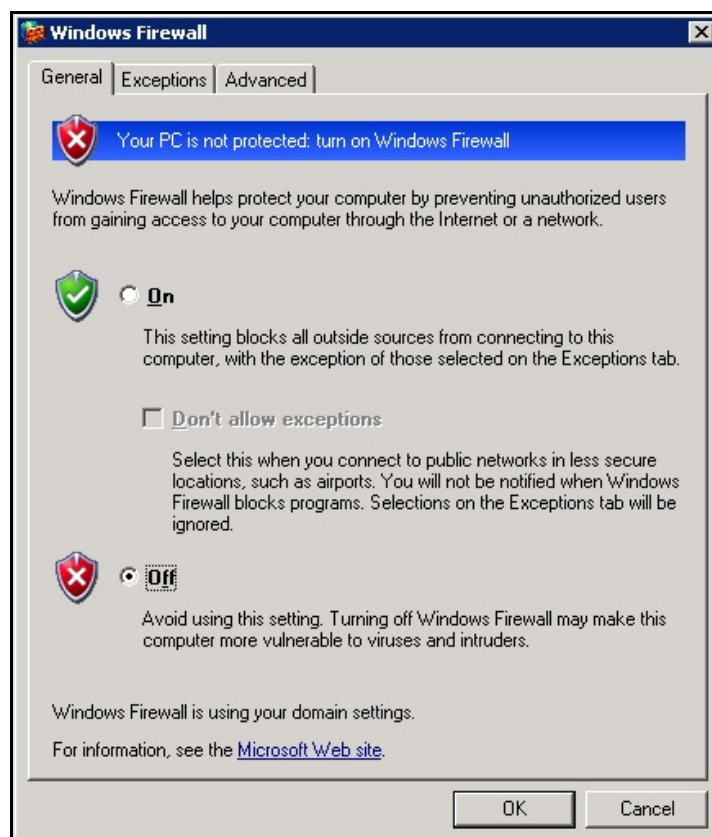


Figure 100 - Turning off Windows Firewall

It is also advisable to **disable the Windows Firewall service** and choose **"Manual" as startup type** in order to avoid the reactivation of the firewall at the next system startup.

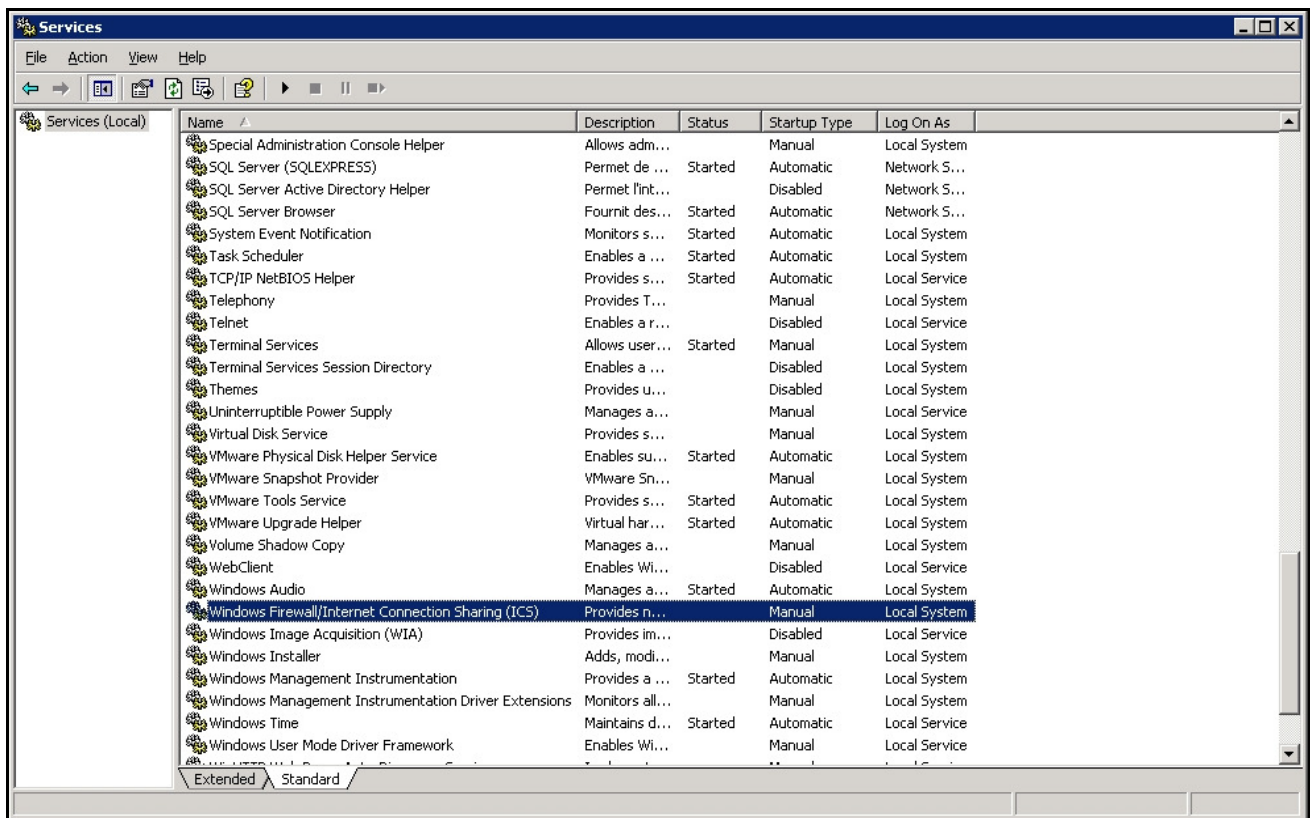


Figure 101 - Windows Firewall/Internet Connection Sharing Service (ICS)

2. Local security policy configuration

From *Start* → *Control Panel* → *Administrative Tools* → *Local Security Policy* menu, select *Local Policies* → *User Rights Assignment*.

From the *Allow log on through Terminal Services* field, specify the group or groups of users allowed to log on to the virtual desktops created from the reference machine.

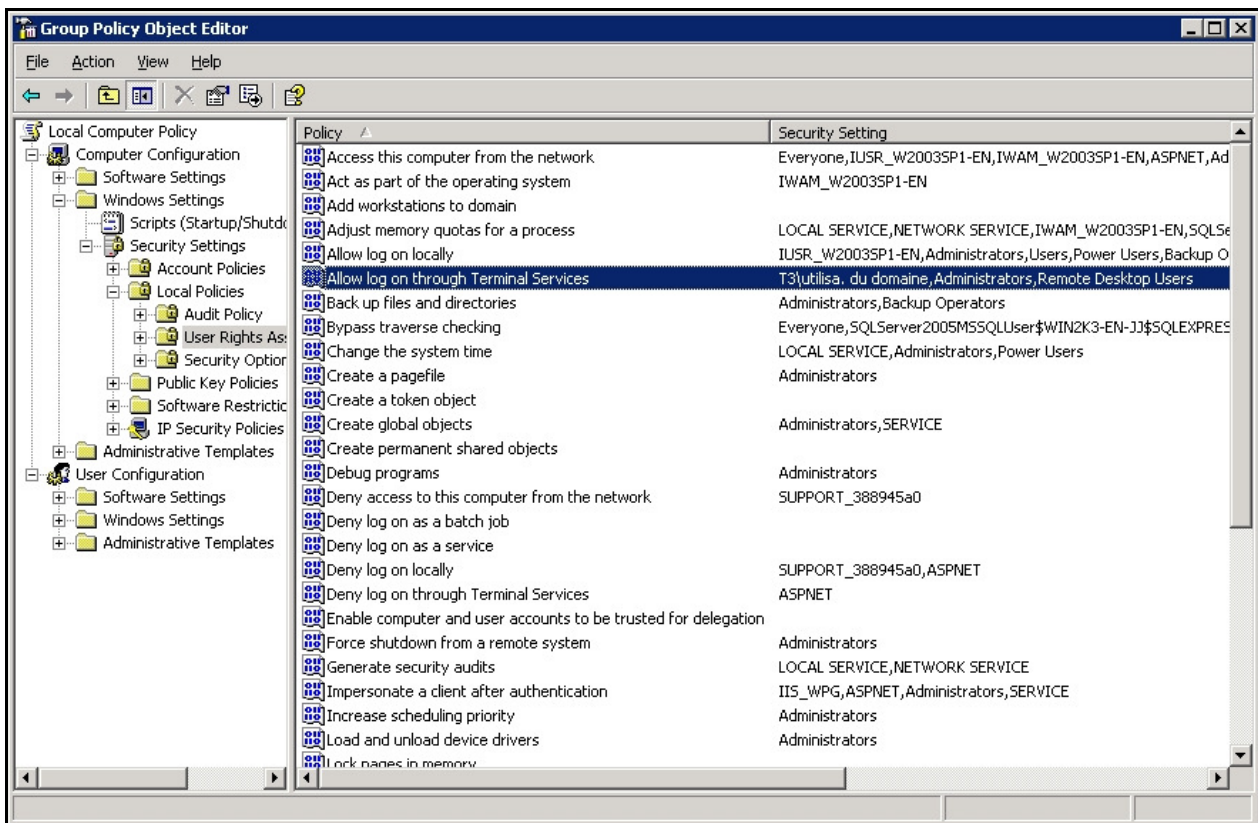


Figure 102 - Allow log on through Terminal Services (GPO)

3. Remote user settings

Right click on *My Computer* and choose *Properties*. From the *Remote* tab, check the *Allow users to connect remotely to this computer* checkbox and click on the *Select Remote Users...* button.

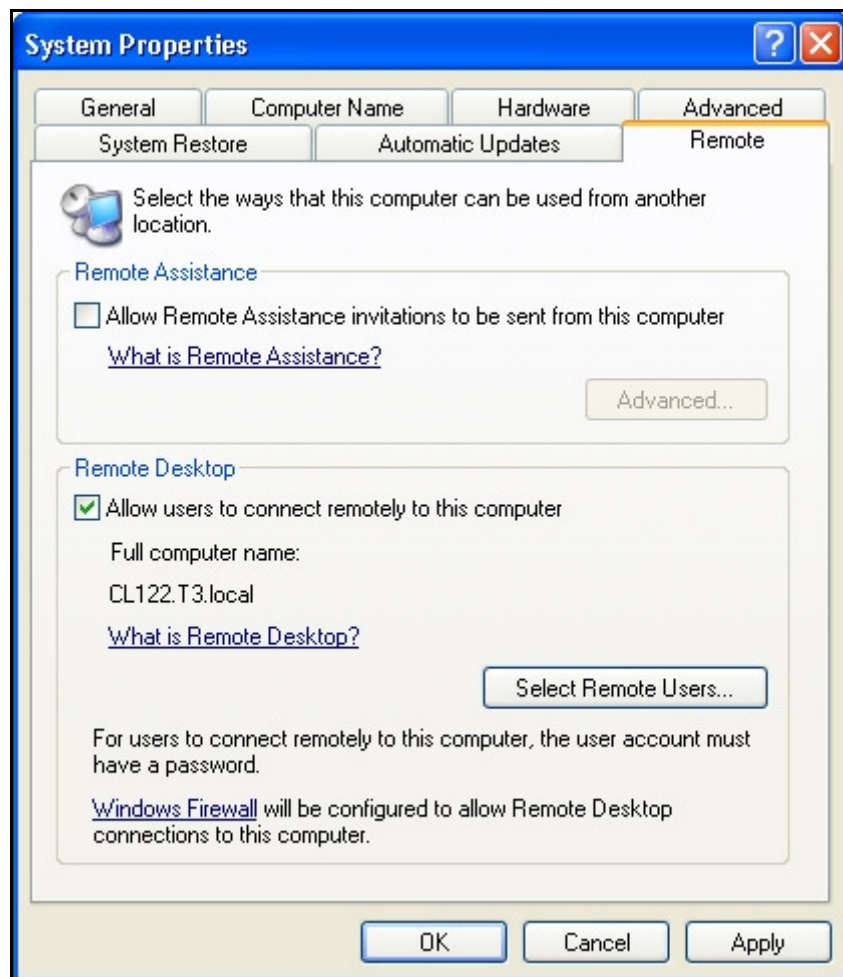


Figure 103 - Computer System Properties (Remote Desktop)

From the *Remote Desktop Users* window, click on the *Add...* button to specify groups of users allowed to log on to the virtual desktops.

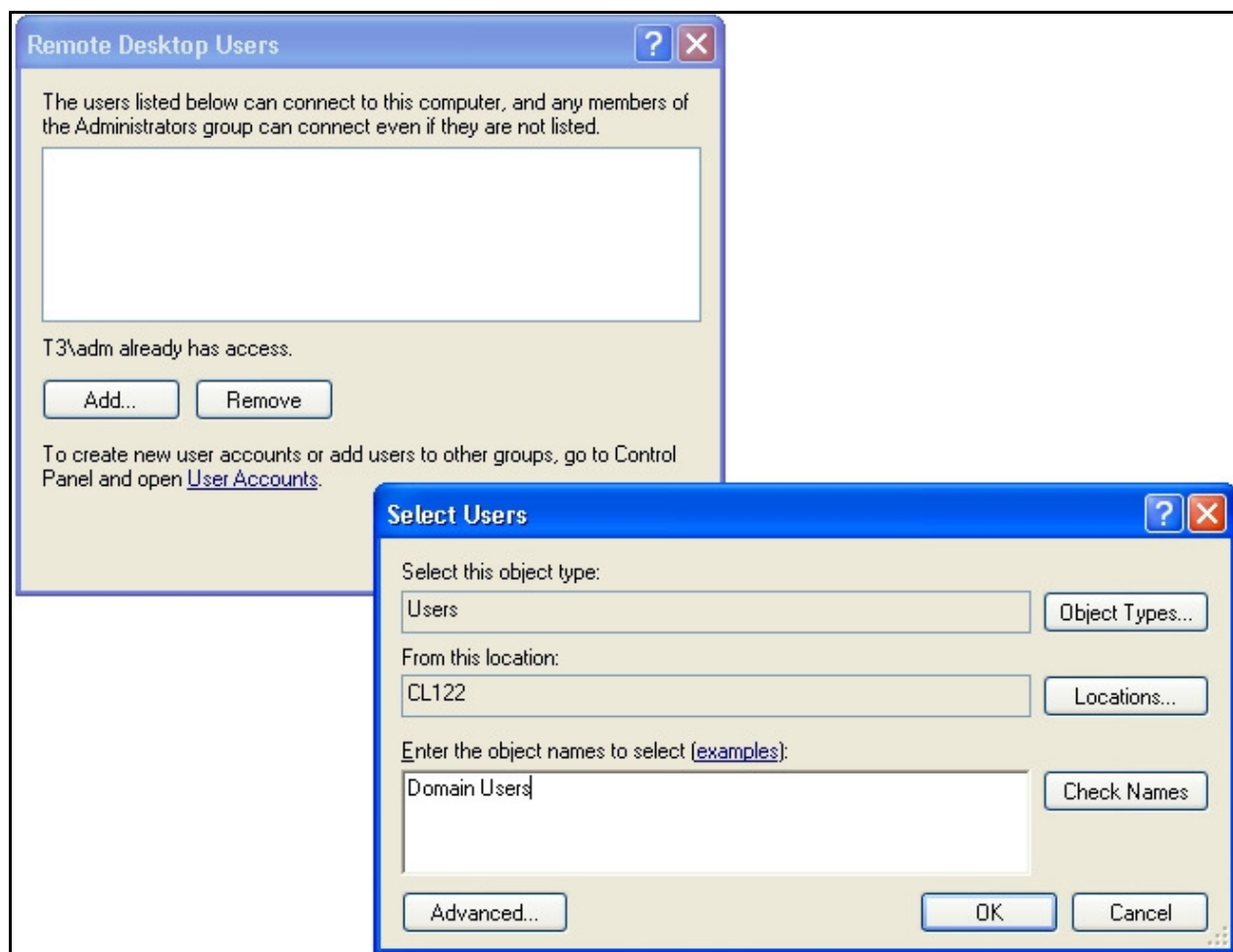


Figure 104 - Add... users to the Remote Desktop Users

4. Remote Registry service

Open the services manager interface (*Start* → *Run* → *services.msc*) and check that *Remote Registry* service is started and its start up type is set as automatic.

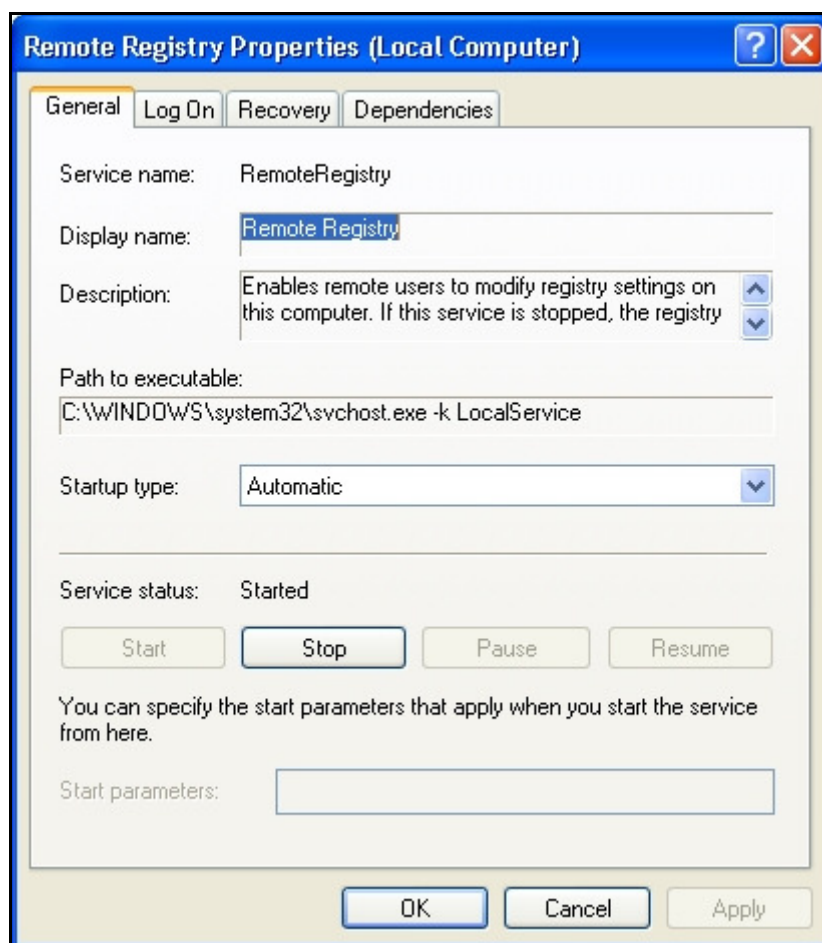


Figure 105 - Remote Registry Properties (Local Computer)

5. Remote Procedure Call (RPC) service

Open the services manager interface (*Start* → *Run* → *services.msc*) and check that *Remote Procedure Call (RPC)* service is started and its start up type is set as automatic.

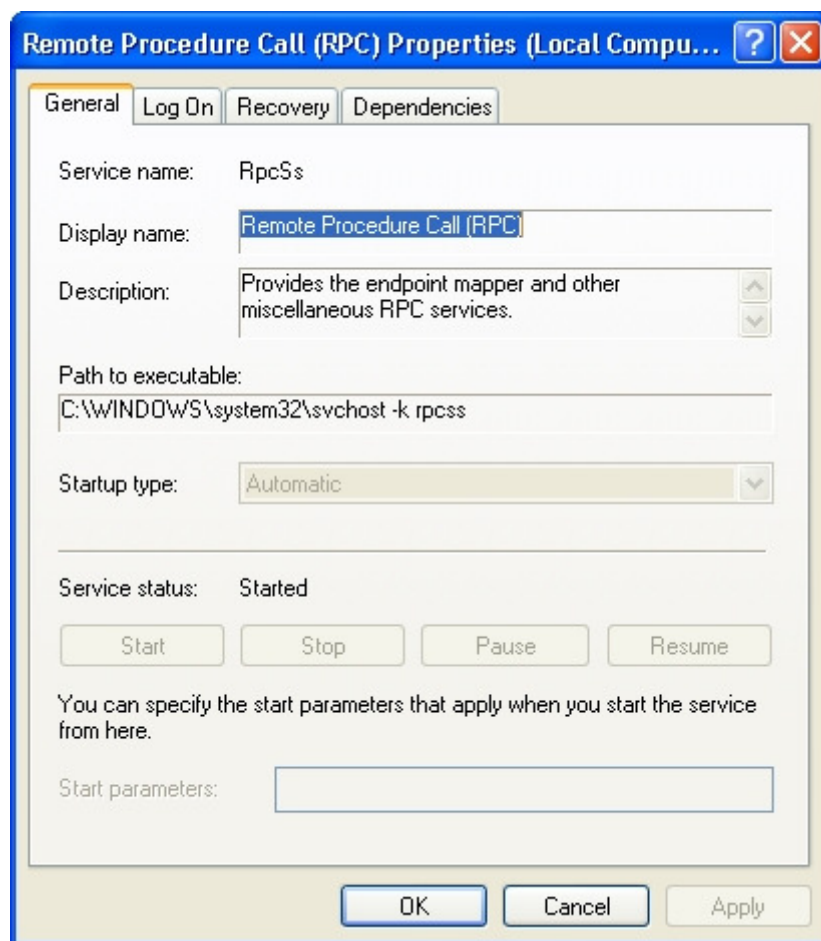


Figure 106 - Remote Procedure Call (RPC) Service

6. **Windows Management Instrumentation (WMI) service**

Open the services manager interface (*Start → Run → services.msc*) and check that *Windows Management Instrumentation* service is started and its start up type is set as automatic.

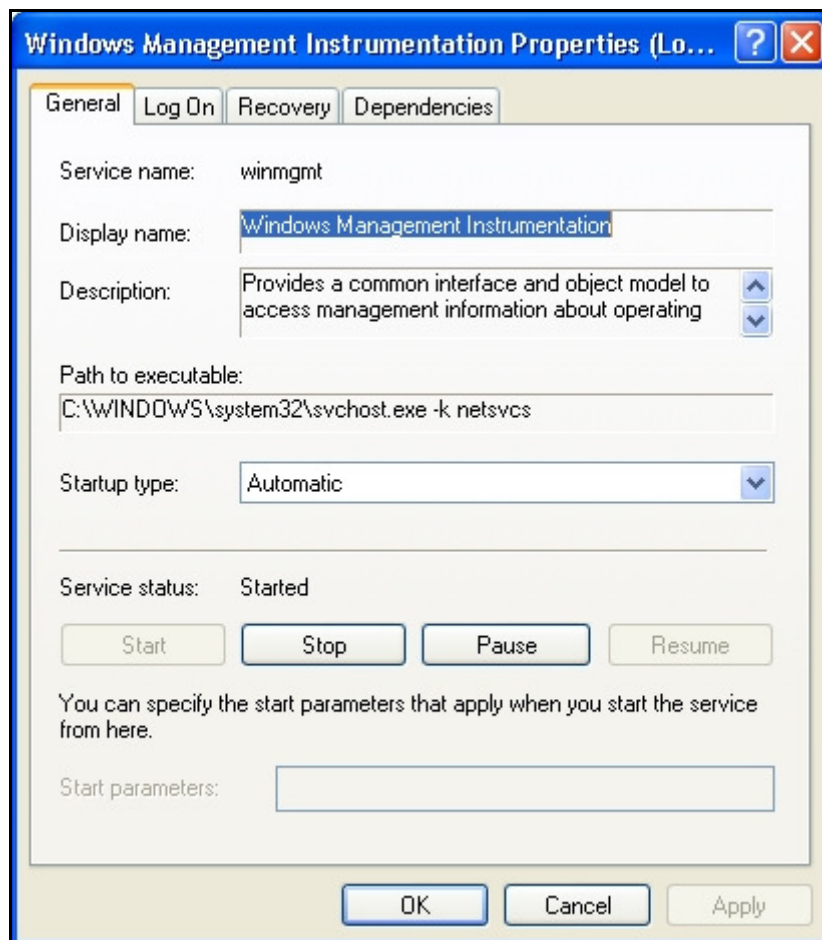


Figure 107 - Windows Management Instrumentation Properties Service

The domain administrator needs to have rights to execute remote WMI requests.

Open the Microsoft Windows Management Infrastructure (WMI) snap-in console (*Start → Run → `wmimgmt.msc`*). Right-click on *WMI Control (local)* and choose *Properties*. From the *WMI Control (Local)* window, select the *Security* tab.

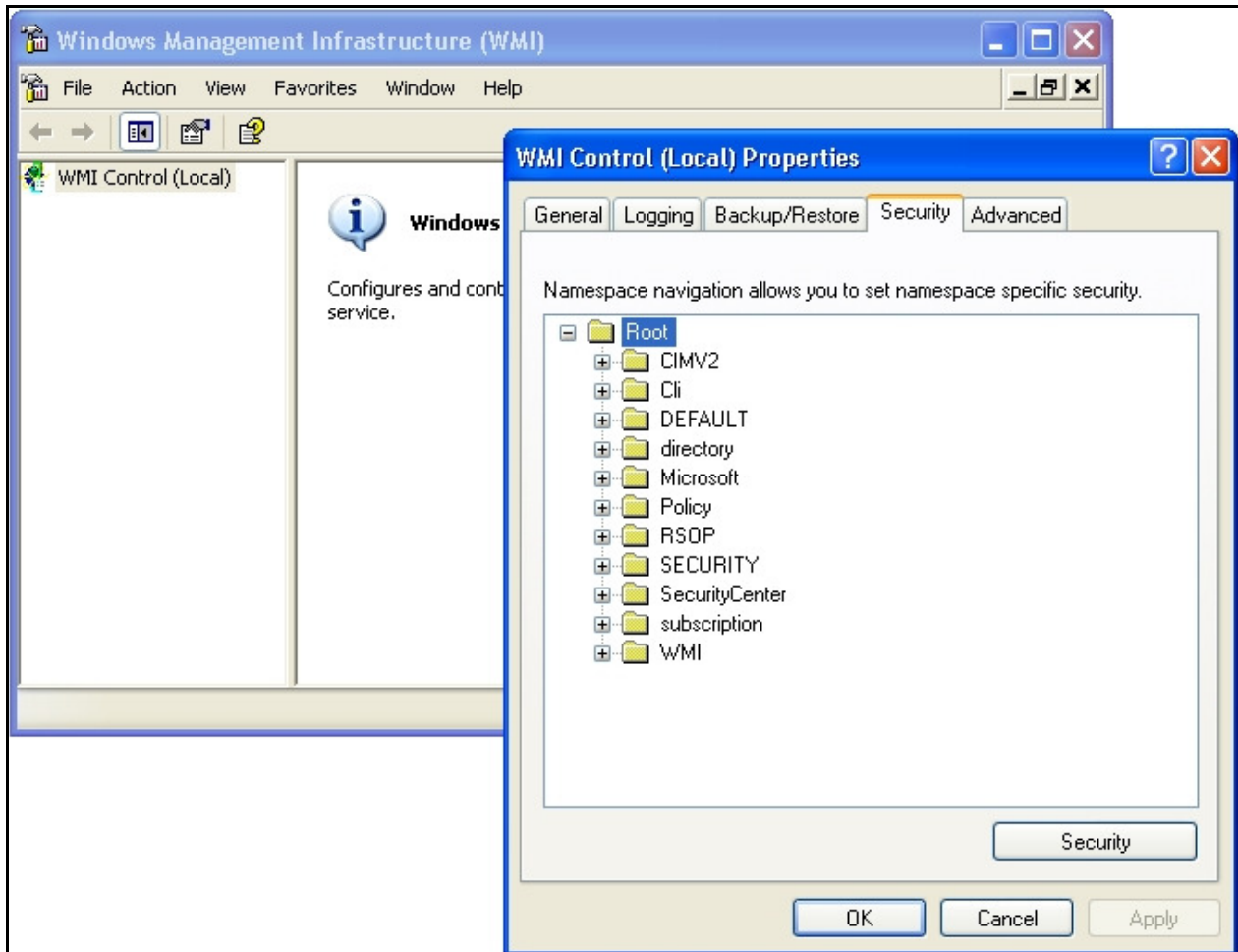


Figure 108 - WMI Control (Local) Properties

Select the *CIMV2* branch and click the *Security* button. Add the domain administrators group allowing all rights (all boxes must be ticked) to the *CIMV2* branch.

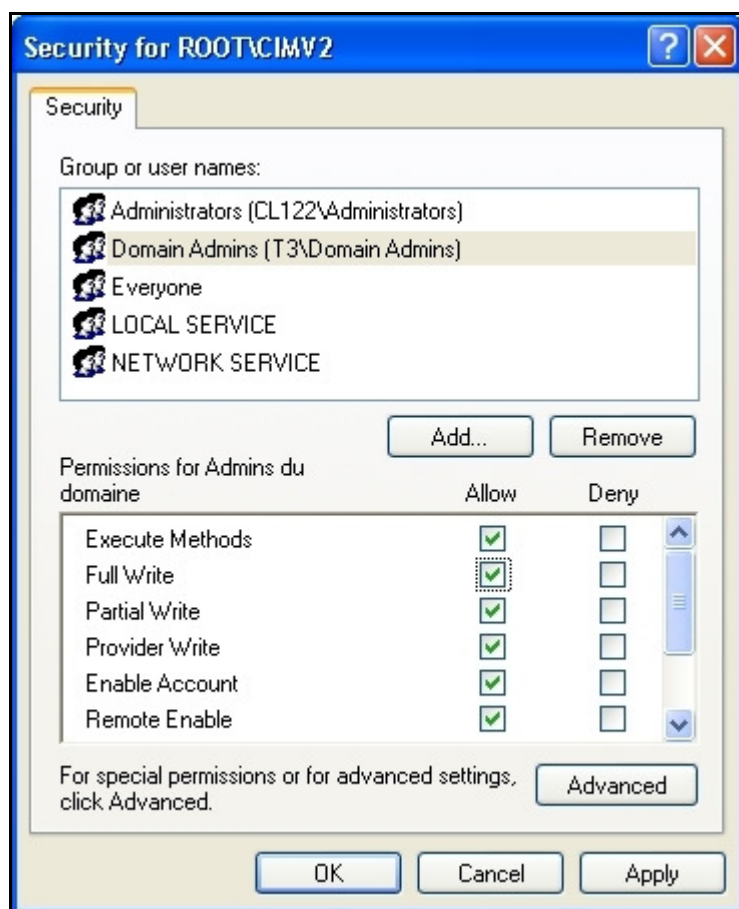


Figure 109 - Security (Permissions for Admins)

7. **COM+ Event System service**

Open the services manager interface (*Start* → *Run* → *services.msc*) and please check that *COM+ Event System* service is started and its start up type is set as automatic

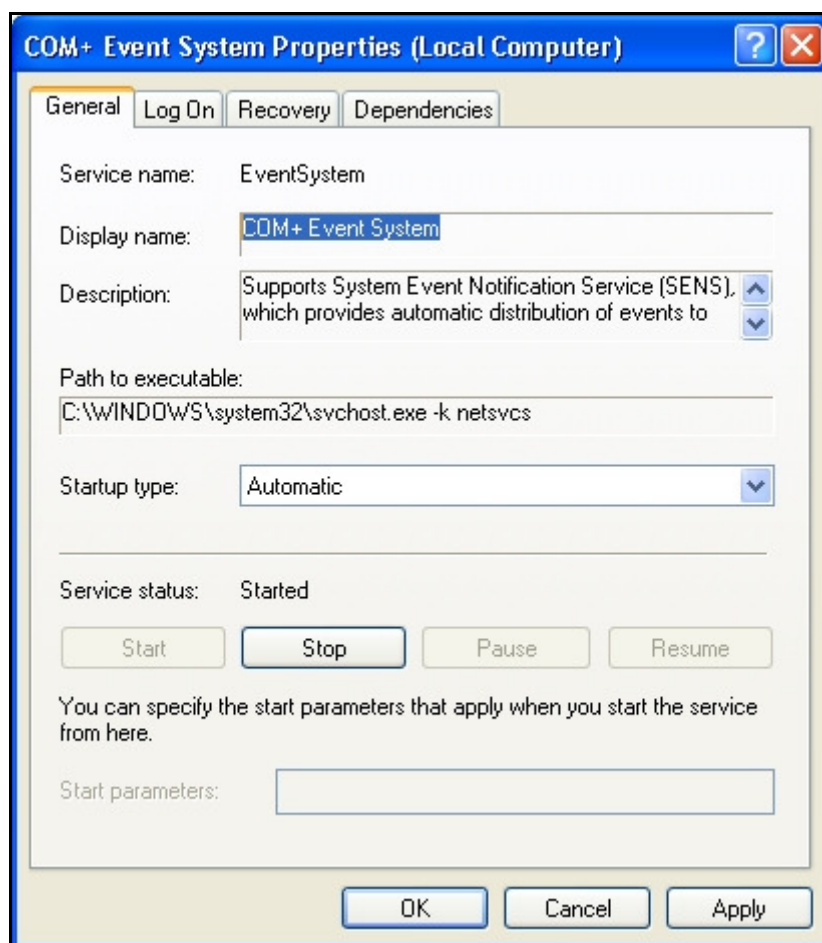


Figure 110 - COM+ Event System Properties Service

8. **VMWare Tools installation**

From the VMWare desktop client, select the virtual machine, click on the *VM* menu and select *Install/Upgrade VMWare Tools*.

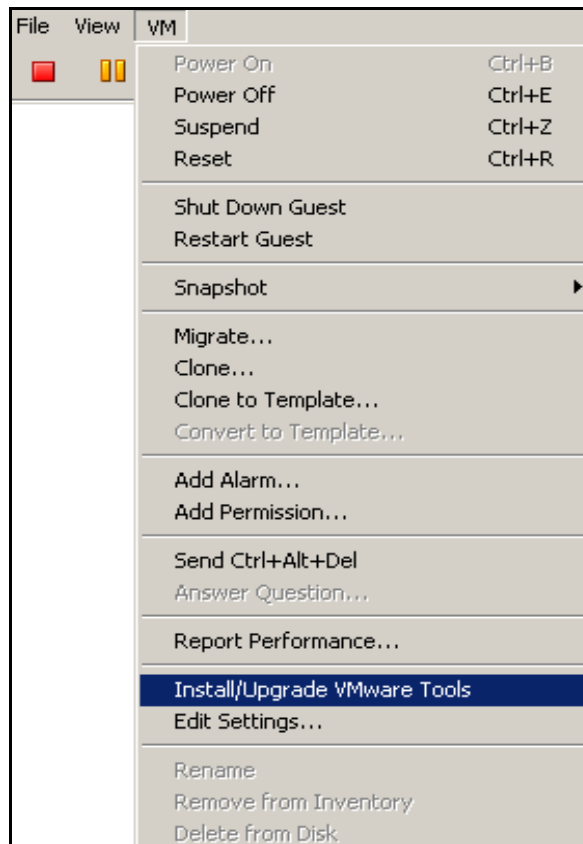


Figure 111 - VMWare Menu (Install/Upgrade VMWare Tools)

This command behaves as if you inserted a CD-ROM to install an application on the virtual machine. If the auto-run of virtual CD-ROM does not run on the virtual machine, open a file explorer instead & double-click on the *VMWare Tools* CD-ROM.

Once the setup is running, follow the steps required to install or upgrade VMWare tools.



Figure 112 - Devices with Removable Storage

7.5 **AppliDis VDI configuration**

AppliDis VDI allows on demand creation, and assignment of virtual machines to desktop or thin client users.

Each virtual machine is stored within a machines pool. When a user makes a request for a virtual machine, the request is passed on to the 'connection-broker' that locates a suitable machine across the list of available machines within the pool. The user then connects to this

machine through Microsoft TSE. This machine can be temporarily or permanently assigned to the user.

This operation requires prior configuration and includes:

1. The choice of a virtual machine to serve as a master on a virtualised host dedicated to the creation of virtual machines. This virtual machine will be cloned according to the size of the pool you want, thus ensuring the consistent configuration of virtual machines within the pool.
2. Associating user groups to machine pools with inherent association rules allowing the 'connection-broker' to assign a desktop to a requesting user.

7.6 AppliDis VDI activation

To activate the AppliDis VDI feature, go to **Configuration → General options** menu and check the **Activate VDI service** checkbox.

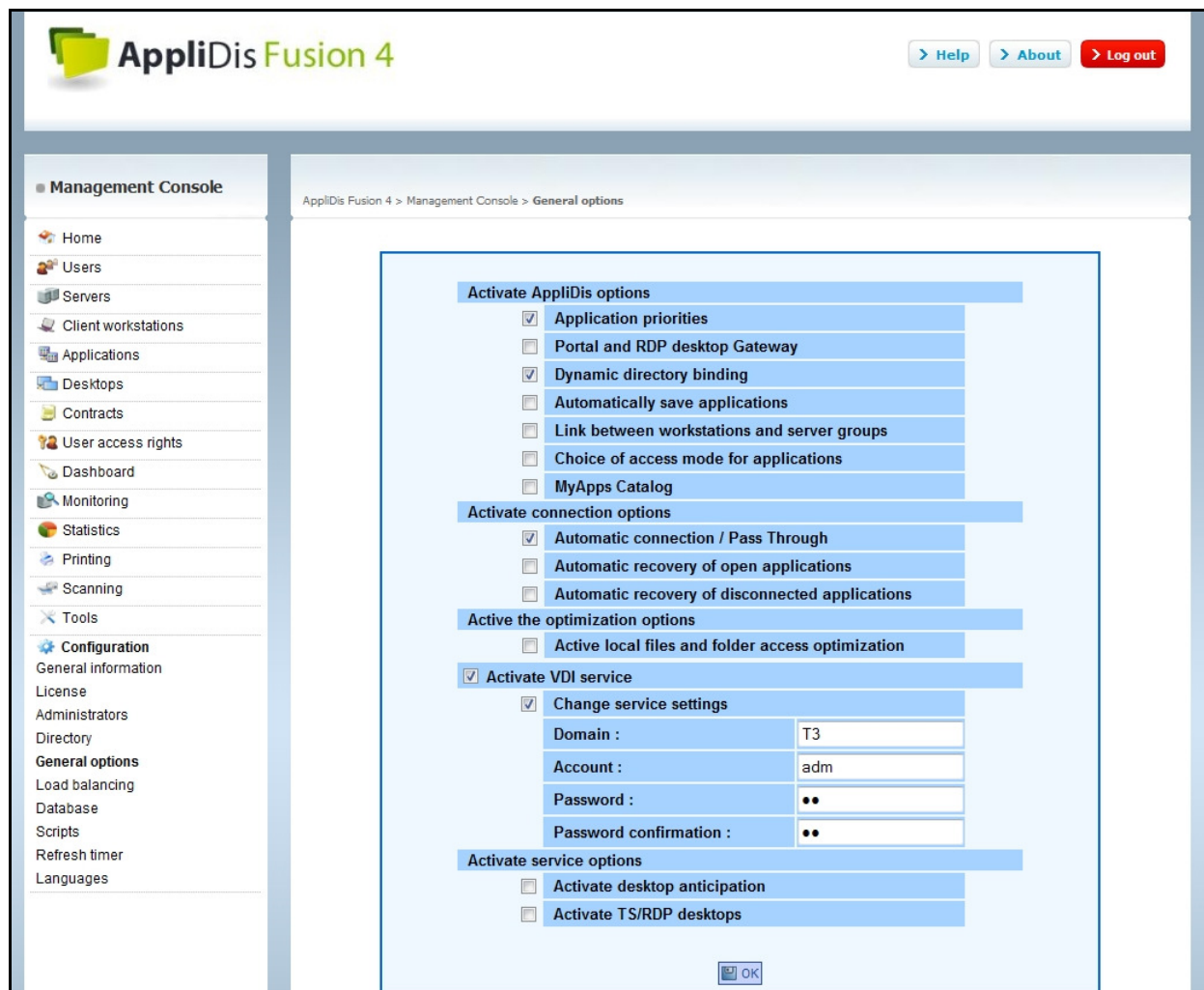


Figure 113 Activate VDI Service (AppliDis Management Console)

Configure the VDI Service settings with a domain administrator account or an account with domain administration privileges.

7.7 How to reference the Virtual machines?

Log on to the AppliDis administration portal and select **Servers** → **Server List** menu.

The screenshot shows the AppliDis Fusion 4 Management Console. The left sidebar contains a 'Management Console' menu with options like Home, Users, Servers, Server list, Server groups, Virtual Machines, Virtual IP configuration, HTTP Gateway, Client workstations, Applications, Desktops, Contracts, User access rights, Dashboard, Monitoring, Statistics, Printing, Scanning, Tools, and Configuration. The main content area shows the 'Server list' page. At the top, there are buttons for 'Add virtual machines host', 'Add Windows servers manually', and 'Add Windows servers automatically'. Below these is a table with the following columns: Server name, Roles, Administration and connection broker, User web portal, Gateway, Application hosts and Windows desktops, and Virtual machines host. The table contains two entries for 'WIN2K3-EN-JJ'. The first entry is marked as an infrastructure server, and the second as a host application and Windows desktops.

Server name	Roles	Administration and connection broker	User web portal	Gateway	Application hosts and Windows desktops	Virtual machines host
WIN2K3-EN-JJ		☒	☒	☒	☒	☐
Total of 1 infrastructure server						
WIN2K3-EN-JJ		☒	☒	☒	☒	☐
Total of 1 host application and Windows desktops						

Figure 114 - Add virtual machines host (AppliDis Management Concole)

Click on the **Add virtual machines host** button to access the **Connection configuration** options.

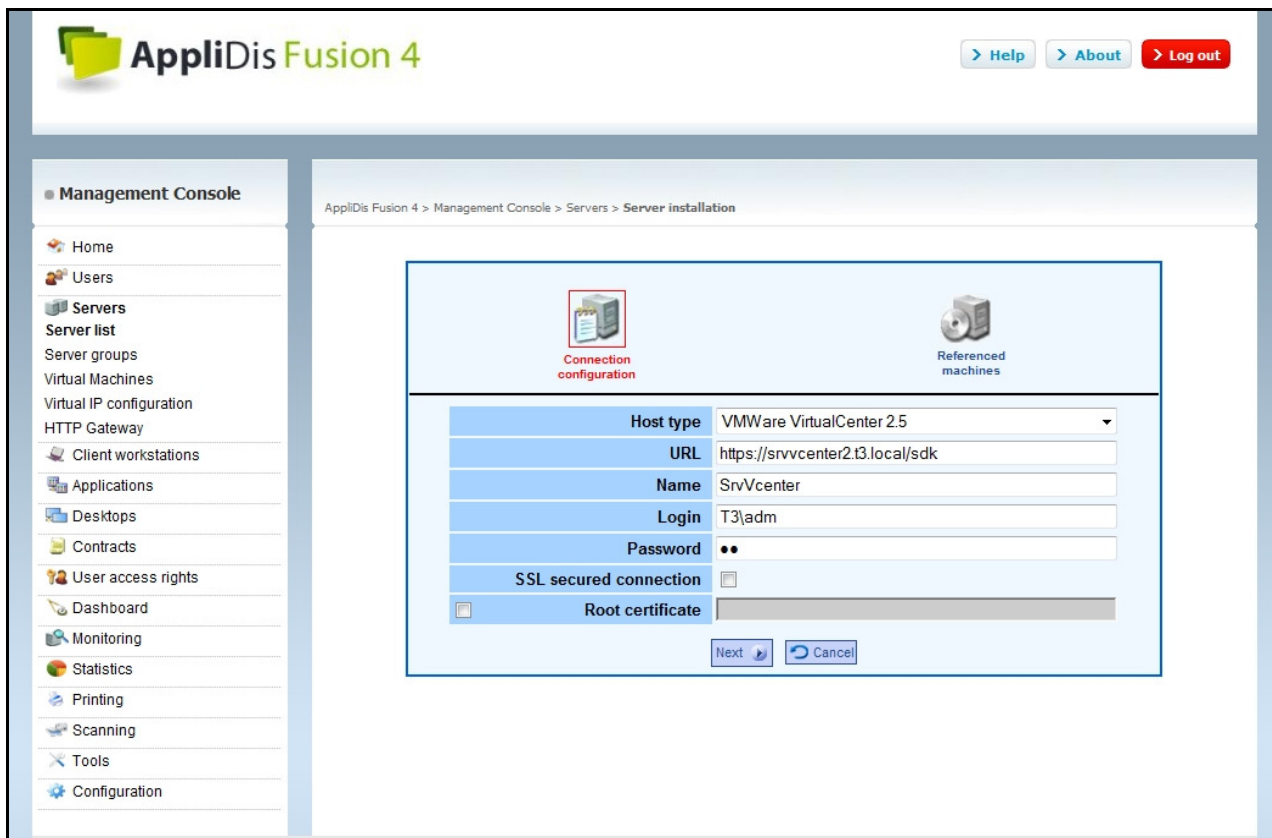


Figure 115 - VDI Connection Configuration (AppliDis Management Console)

Please select the host type, and enter:

1. The connection URL of a VMWare VirtualCenter server. The format of the URL is:
http://{ip or name of VirtualCenter server}/sdk

or

https://{ip or name of VirtualCenter server}/sdk

and for Microsoft Hyper V, ***The IP address or the FQDN of Microsoft Hyper V server***

2. The Server name. This name describes the host as you would like it to appear in the server list, and can be different from the actual Host name.
3. A domain administrator account, or an account with domain administrator privileges.
4. The password of the domain account.
5. If appropriate, please provide SSL information (if a secure certified connection has been configured).

And, then, click on the **Next** button.

AppliDis will automatically enumerate the list of virtual machines managed by the VMWare vCenter or Hyper V Hosts.

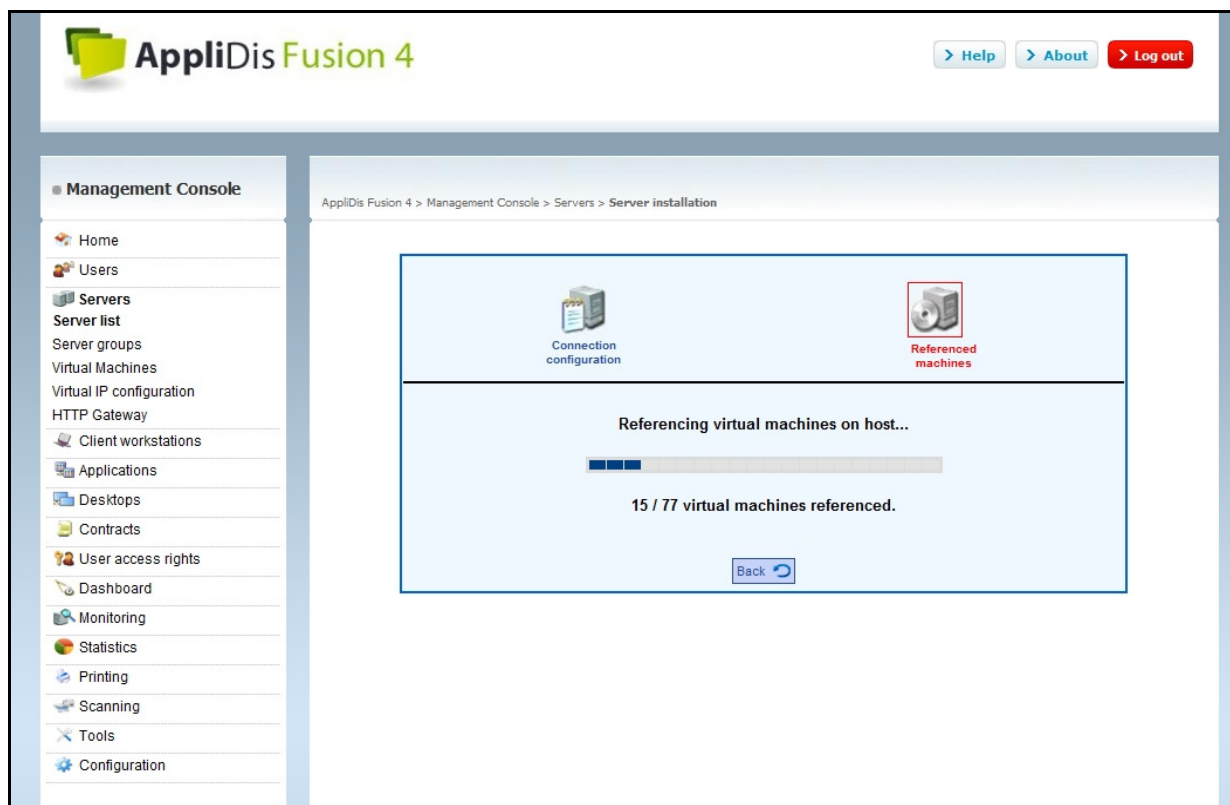


Figure 116 - Referencing virtual machines on host... (Management Console)

When the enumeration process has terminated, a list of available machines is now displayed. Click on the **Back** button.

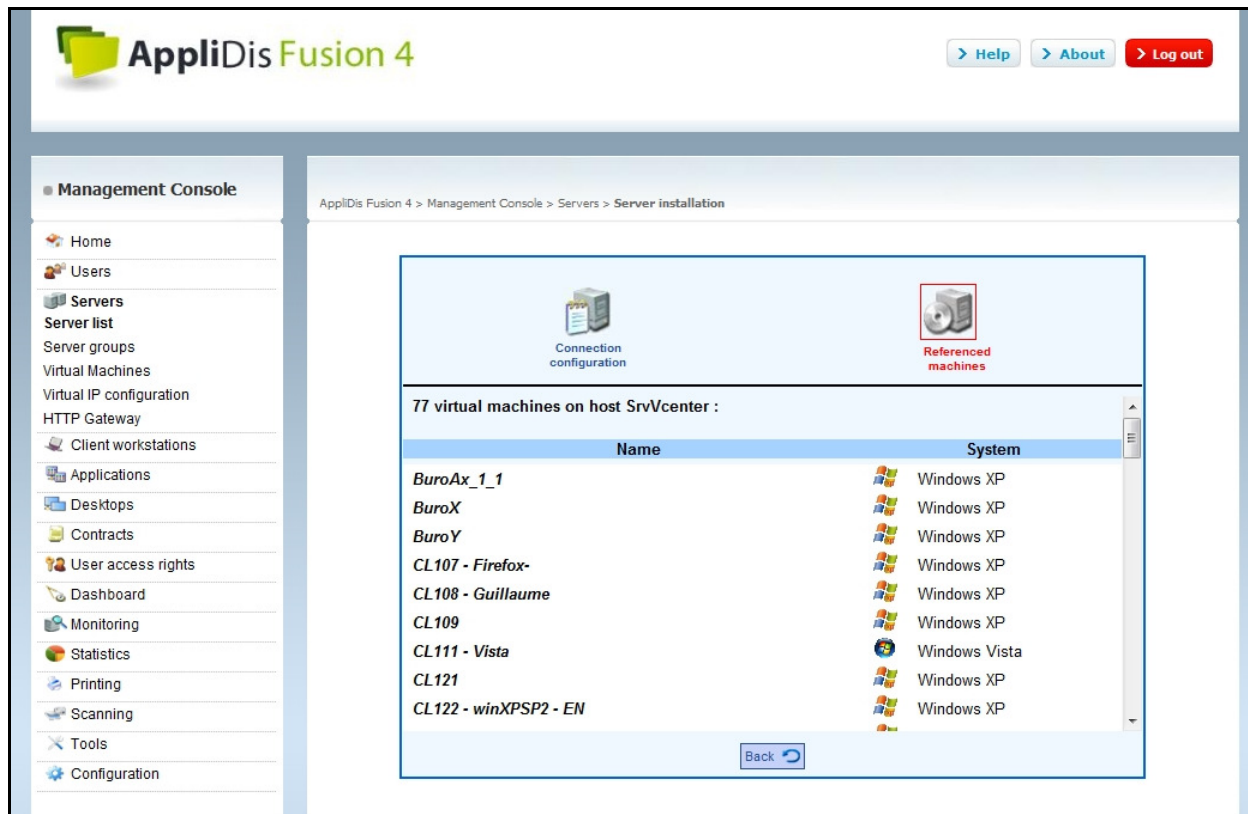


Figure 117 - Virtual machines on host SrvVcenter (AppliDis Management Console)

You will be returned to the server list. The VDI host you have just added now appears within the **virtual machines host** list (SrvVCenter at the bottom of the screenshot below).

AppliDis Fusion 4 Management Console

AppliDis Fusion 4 > Management Console > Servers > Server list

Server list

Server groups

Virtual Machines

Virtual IP configuration

HTTP Gateway

Client workstations

Applications

Desktops

Contracts

User access rights

Dashboard

Monitoring

Statistics

Printing

Scanning

Tools

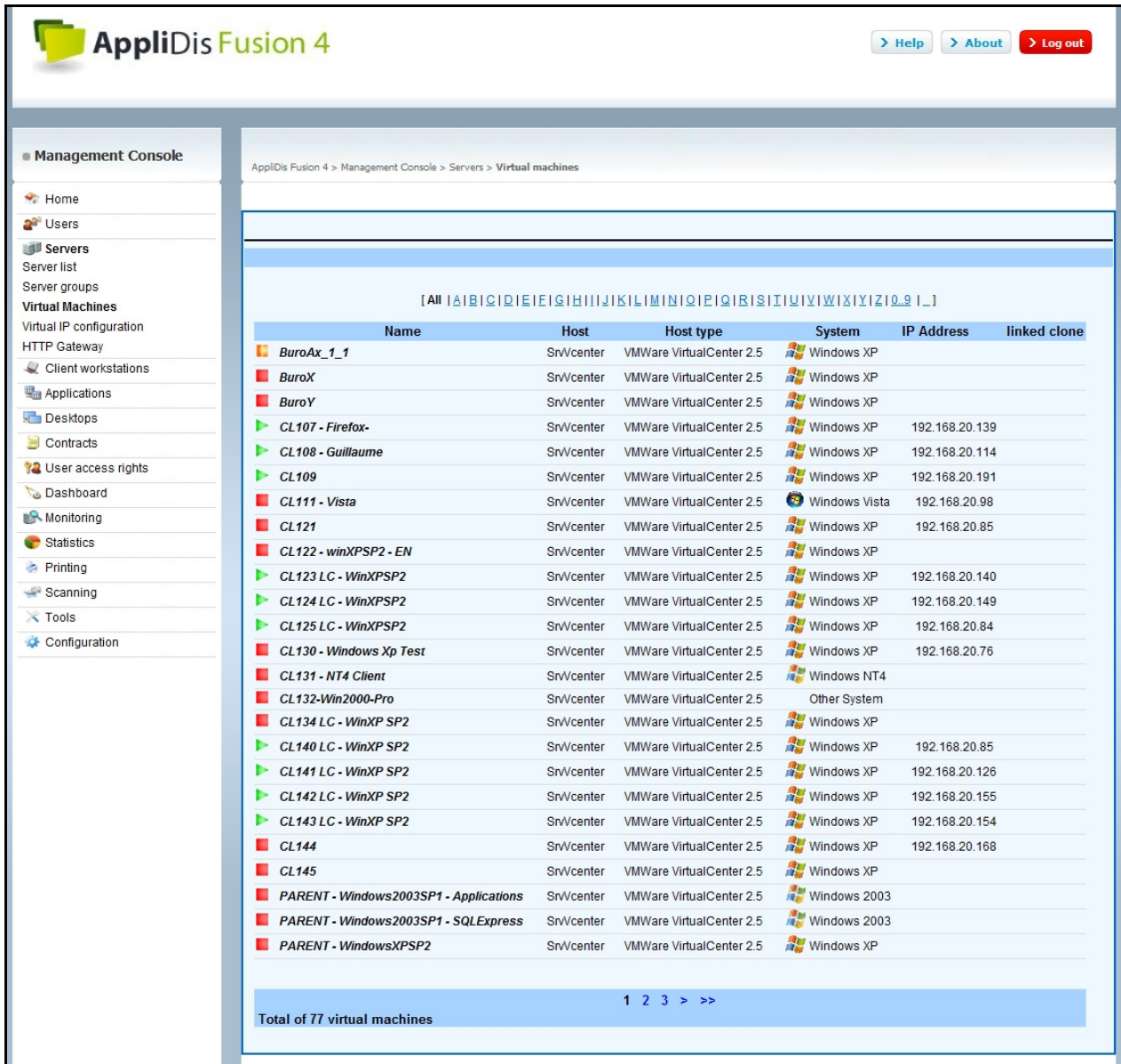
Configuration

Server list table:

Server name	Roles : Administration and connection broker	User web portal	Gateway	Application hosts and Windows desktops	Virtual machines host
WIN2K3-EN-JJ	☒	☒	☒	☒	☐
Total of 1 infrastructure server					
WIN2K3-EN-JJ	☒	☒	☒	☒	☐
Total of 1 host application and Windows desktops					
SrvVcenter	☐	☐	☐	☐	☒
Total of 1 virtuals machines host					

Figure 118 - Virtual Machine Host in the Server list (AppliDis Management Console)

The list of available virtual machines now appears in the **Servers → Virtual Machines** menu.



The screenshot displays the AppliDis Fusion 4 Management Console interface. The left sidebar shows the navigation menu with the 'Virtual Machines' option selected. The main content area displays a table of 27 virtual machines. The table has columns for Name, Host, Host type, System, IP Address, and linked clone. The machines are listed with various names like BuroAx_1_1, BuroX, BuroY, CL107 - Firefox-, CL108 - Guillaume, CL109, CL111 - Vista, CL121, CL122 - winXPSP2 - EN, CL123 LC - WinXPSP2, CL124 LC - WinXPSP2, CL125 LC - WinXPSP2, CL130 - Windows Xp Test, CL131 - NT4 Client, CL132-Win2000-Pro, CL134 LC - WinXP SP2, CL140 LC - WinXP SP2, CL141 LC - WinXP SP2, CL142 LC - WinXP SP2, CL143 LC - WinXP SP2, CL144, CL145, PARENT - Windows2003SP1 - Applications, PARENT - Windows2003SP1 - SQLExpress, and PARENT - WindowsXPSP2. The table is filtered by 'All' and shows a total of 77 virtual machines.

Name	Host	Host type	System	IP Address	linked clone
BuroAx_1_1	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP		
BuroX	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP		
BuroY	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP		
CL107 - Firefox-	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.139	
CL108 - Guillaume	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.114	
CL109	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.191	
CL111 - Vista	SrvVcenter	VMWare VirtualCenter 2.5	Windows Vista	192.168.20.98	
CL121	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.85	
CL122 - winXPSP2 - EN	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP		
CL123 LC - WinXPSP2	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.140	
CL124 LC - WinXPSP2	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.149	
CL125 LC - WinXPSP2	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.84	
CL130 - Windows Xp Test	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.76	
CL131 - NT4 Client	SrvVcenter	VMWare VirtualCenter 2.5	Windows NT4		
CL132-Win2000-Pro	SrvVcenter	VMWare VirtualCenter 2.5	Other System		
CL134 LC - WinXP SP2	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP		
CL140 LC - WinXP SP2	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.85	
CL141 LC - WinXP SP2	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.126	
CL142 LC - WinXP SP2	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.155	
CL143 LC - WinXP SP2	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.154	
CL144	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP	192.168.20.168	
CL145	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP		
PARENT - Windows2003SP1 - Applications	SrvVcenter	VMWare VirtualCenter 2.5	Windows 2003		
PARENT - Windows2003SP1 - SQLExpress	SrvVcenter	VMWare VirtualCenter 2.5	Windows 2003		
PARENT - WindowsXPSP2	SrvVcenter	VMWare VirtualCenter 2.5	Windows XP		

Total of 77 virtual machines

Figure 119 - Available Virtual machines (AppliDis Management Console)

7.8 Configuration of a machine reference

For further information on reference machines, please refer to the « **Prerequisites for VDI desktops creation** » document.

7.9 Creation of a desktop pools

Automatic creation from a machine reference

Within the AppliDis administration portal, access to **Desktops** → **Desktops list** menu.

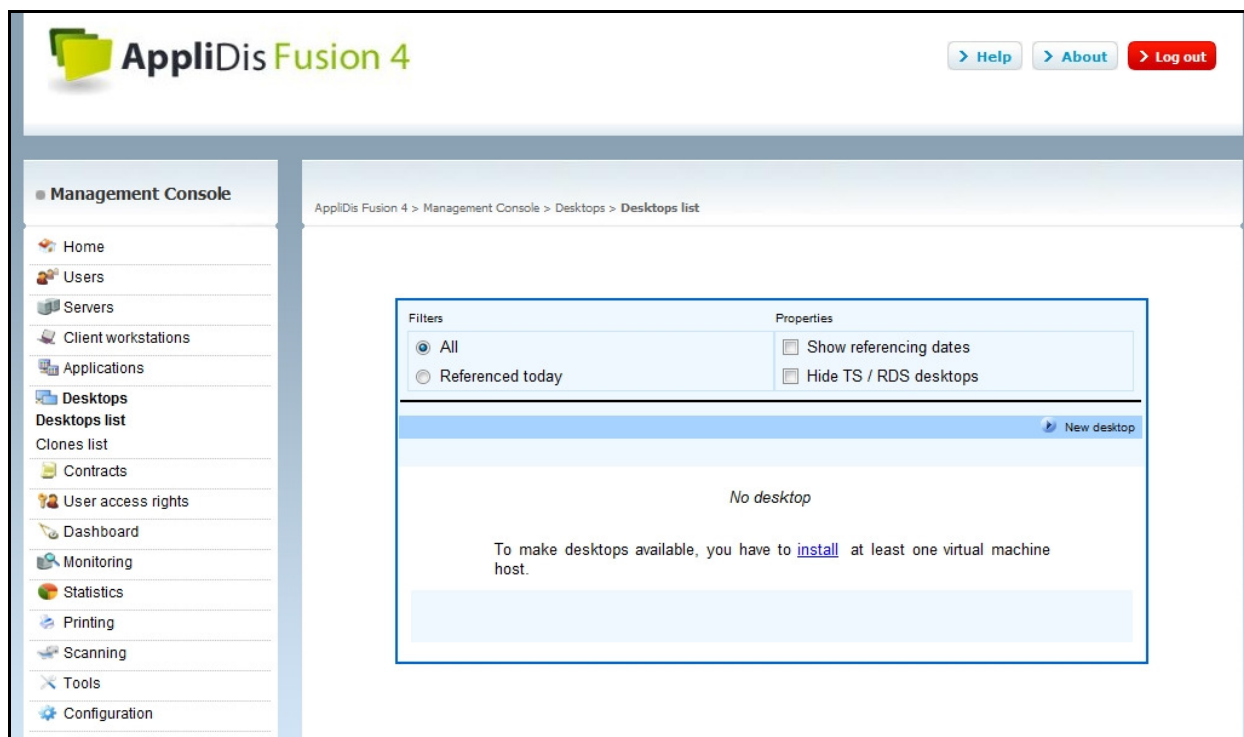


Figure 120 - Desktop list (AppliDis Management Console)

And then, click on the **New desktop** button.

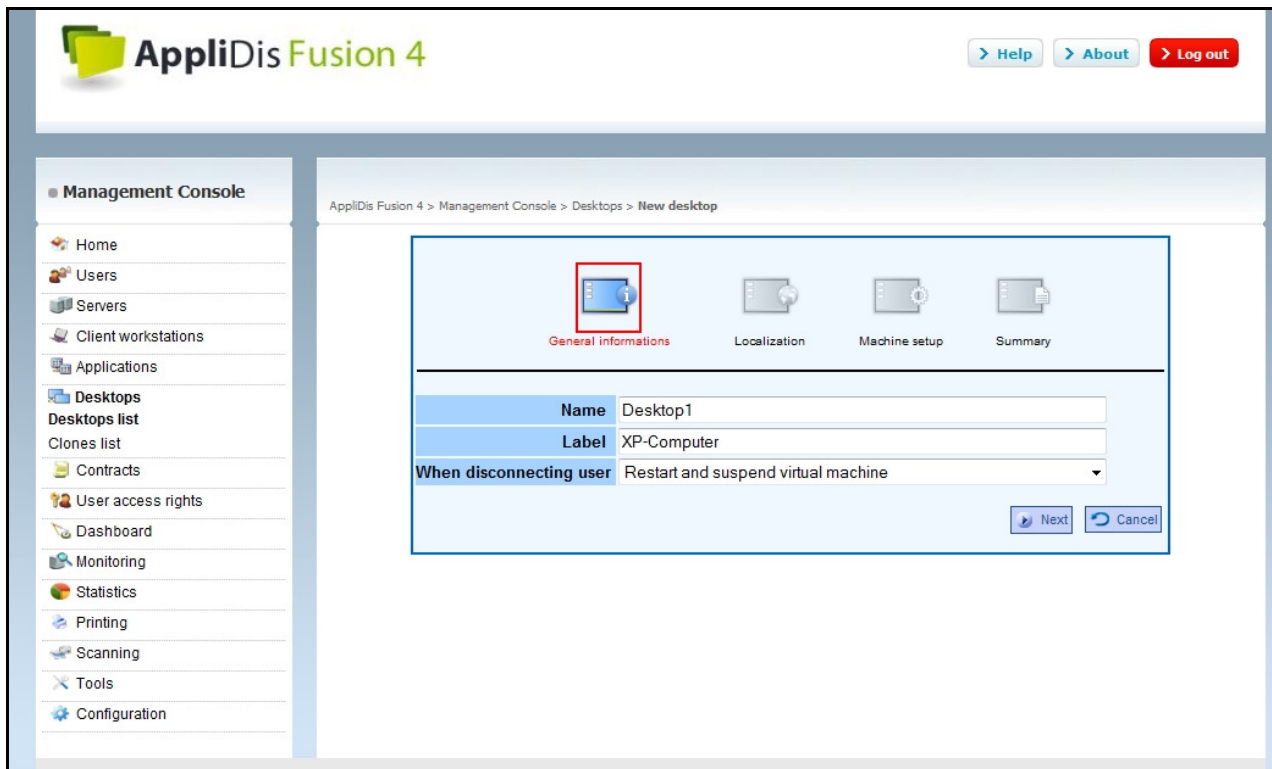


Figure 121 - New Desktop (AppliDis Management Console)

Specify a unique name and a label for the desktop pool to create.

Note: The pool label is displayed in the client web interface and identifies the virtual desktop. The unique name is not displayed to users.

Choose an action to perform when a user closes his desktop:

- Restart and suspend virtual machine,
- Stop virtual machine,
- Restart the virtual machine.

And then, click on the **Next** button.

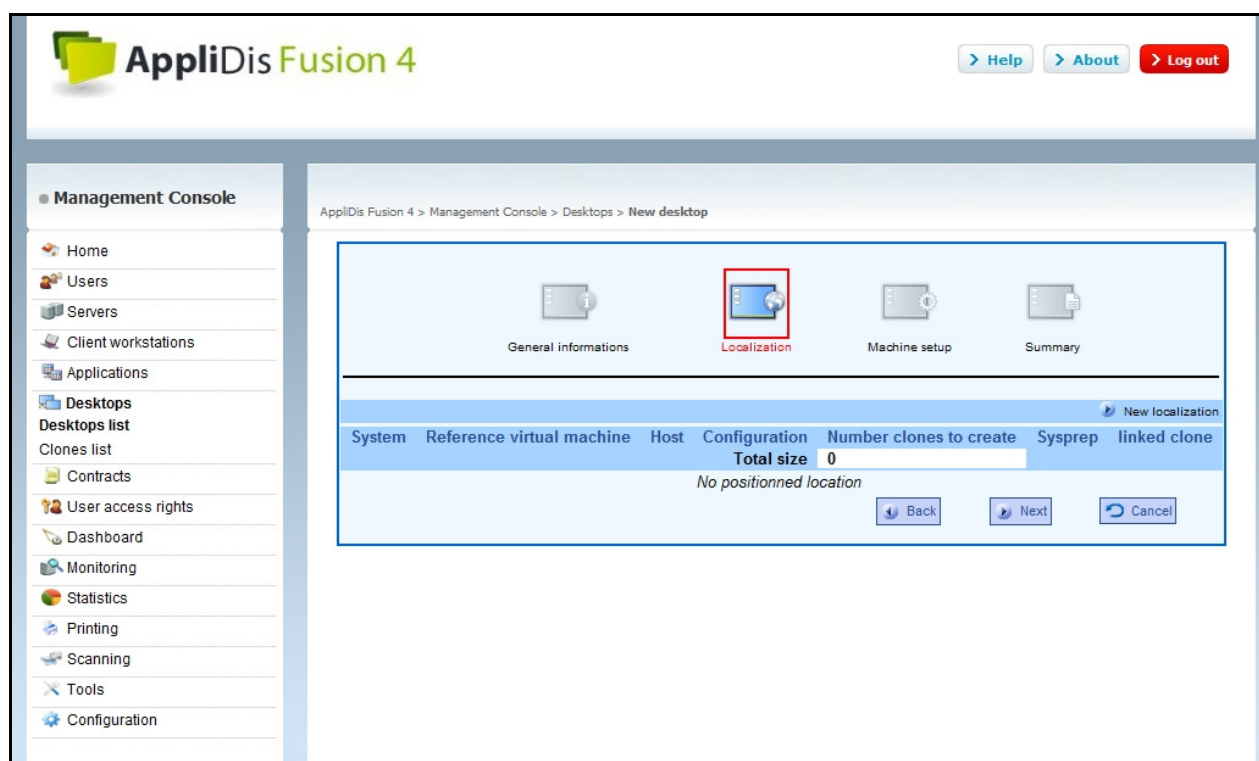


Figure 122 - Localization, New Desktops (AppliDis Management Console)

And then, click on the **New localization** button.

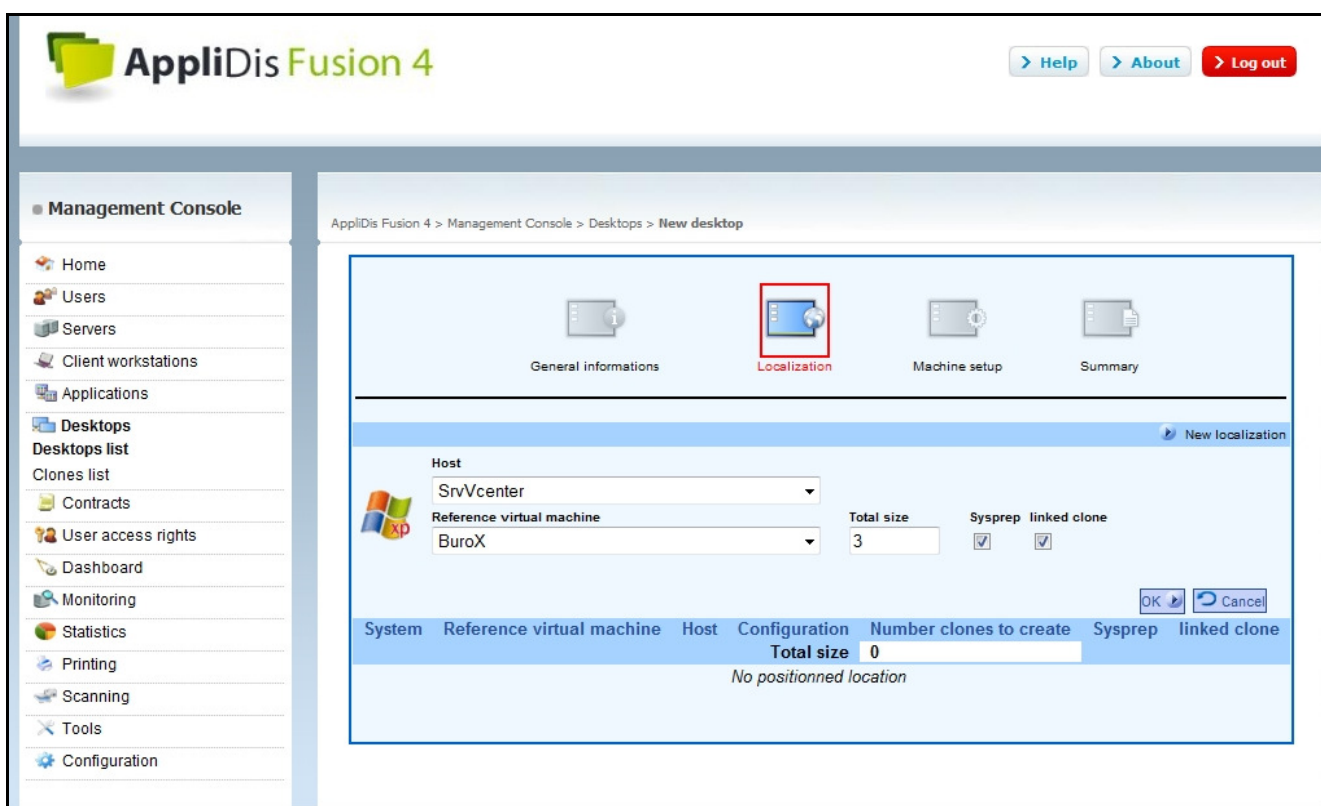


Figure 123 - Host & Reference virtual machine (AppliDis Management Console)

The graphical interface allows Host and virtual machine selection among the available machines registered with AppliDis VDI, the size of the pool, what type of clone, and whether the machine should be syspreped.

Enter:

- The Host server where the reference machine is located.
- The name of the reference machine.
- The size of the pool to create (number of desktops to create by cloning the reference machine).
- Specify if the desktops require system configuration using the sysprep tool.
- Specify the clone type (if this option is not selected a full clone will be created)

Click on the **OK** button.

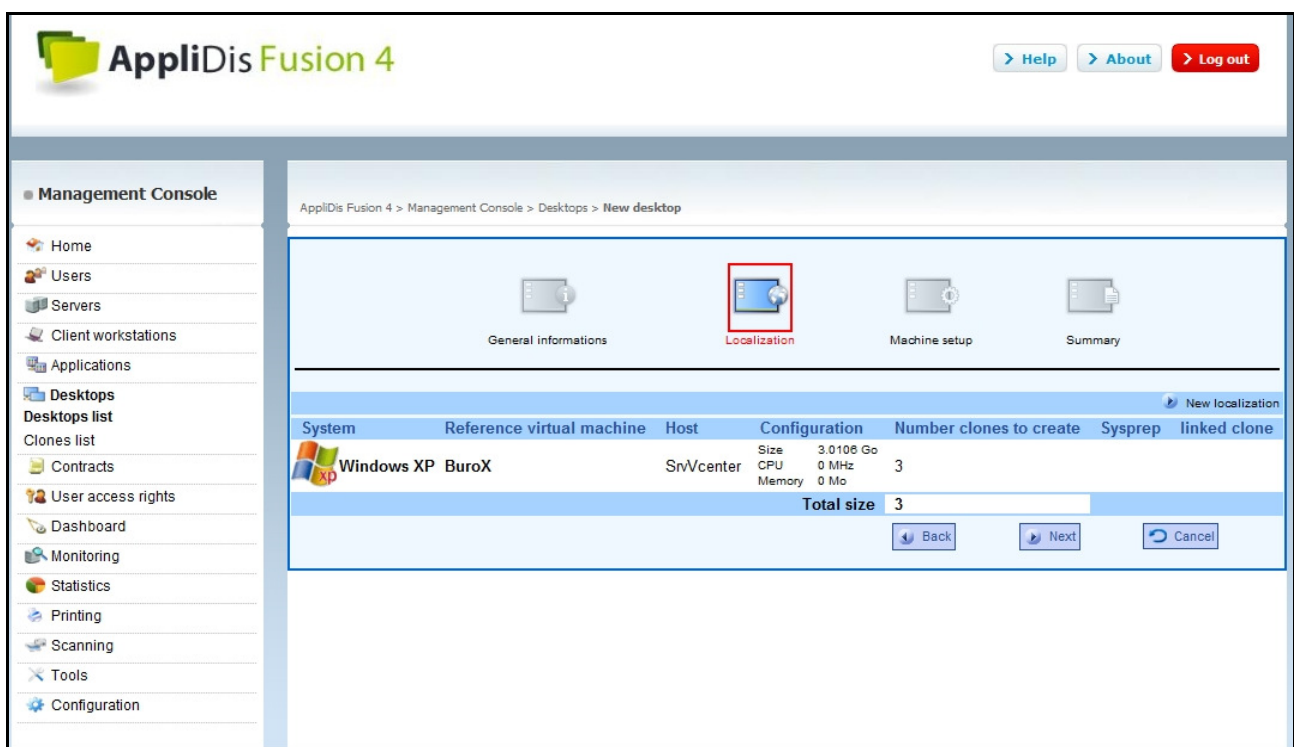


Figure 124 - Reference virtual machine (AppliDis Management Console)

The newly referenced machine now appears within the list of machines. Follow the above procedure if you wish to add other reference machines.

Select the reference machines you want to create and click on the **Next** button.

The screenshot shows the AppliDis Fusion 4 Management Console interface. The left sidebar contains a 'Management Console' menu with various options like Home, Users, Servers, Client workstations, Applications, Desktops, Desktops list, Clones list, Contracts, User access rights, Dashboard, Monitoring, Statistics, Printing, Scanning, Tools, and Configuration. The main area displays the 'New desktop' wizard. The 'Machine setup' step is highlighted with a red box. It includes fields for 'Name' (Desktop1) and 'Label' (XP-Computer). Below these are fields for 'Domain' (T3), 'Domain administrator account' (adm), 'Password', 'Retype the password', 'Password of the local administrator account (virtual machine)', and 'Retype the local password'. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.

Figure 125 - Machine setup (AppliDis Management Console)

This graphical interface allows you to provide account information needed to finalize desktop creation.

Enter:

1. The domain name corresponding to the reference machine and the resulting desktops to be created.
2. An account name with domain administrator's rights.
3. The password of the domain administrator's account.
4. The password of the local administrators account on the desktops to be created.

And then, click on the **Next** button.

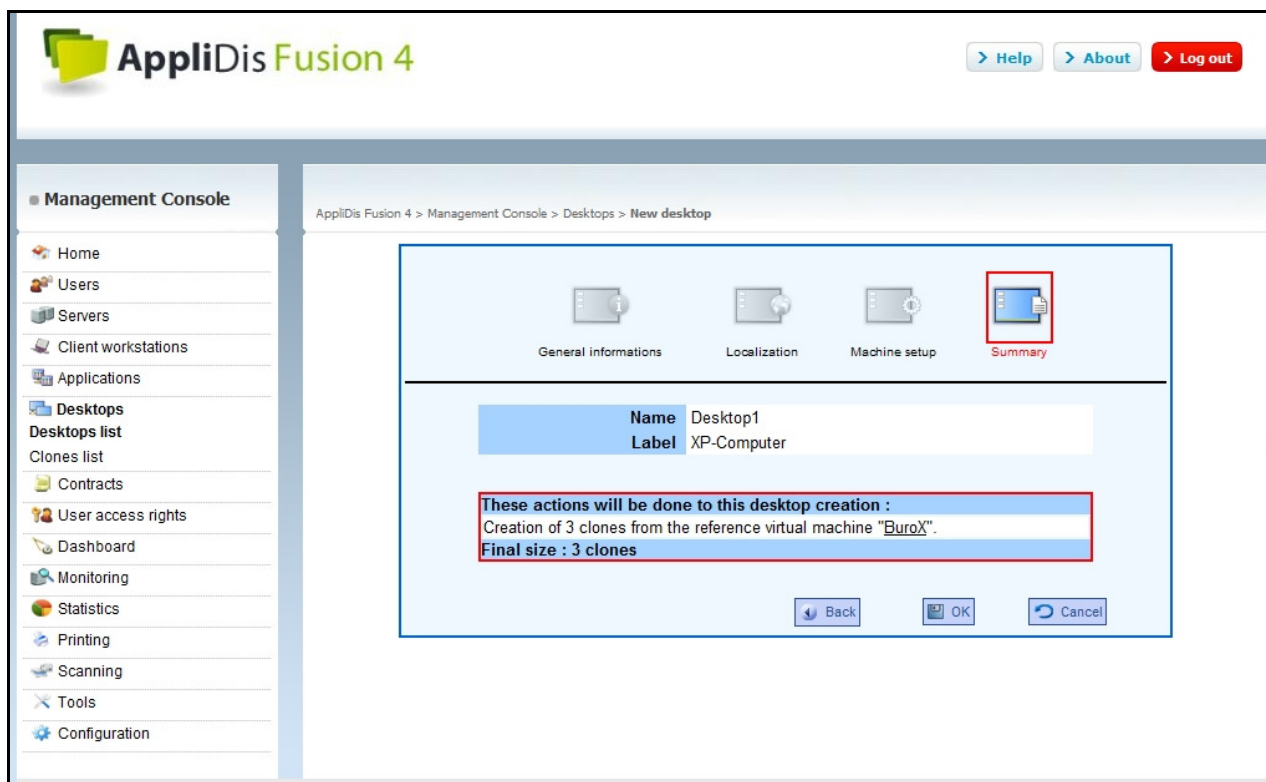


Figure 126 - Desktops list summary (AppliDis Management Console)

The summary page, summarizes the information previously entered for this pool. Click on the **OK** button to start the desktop creation process.

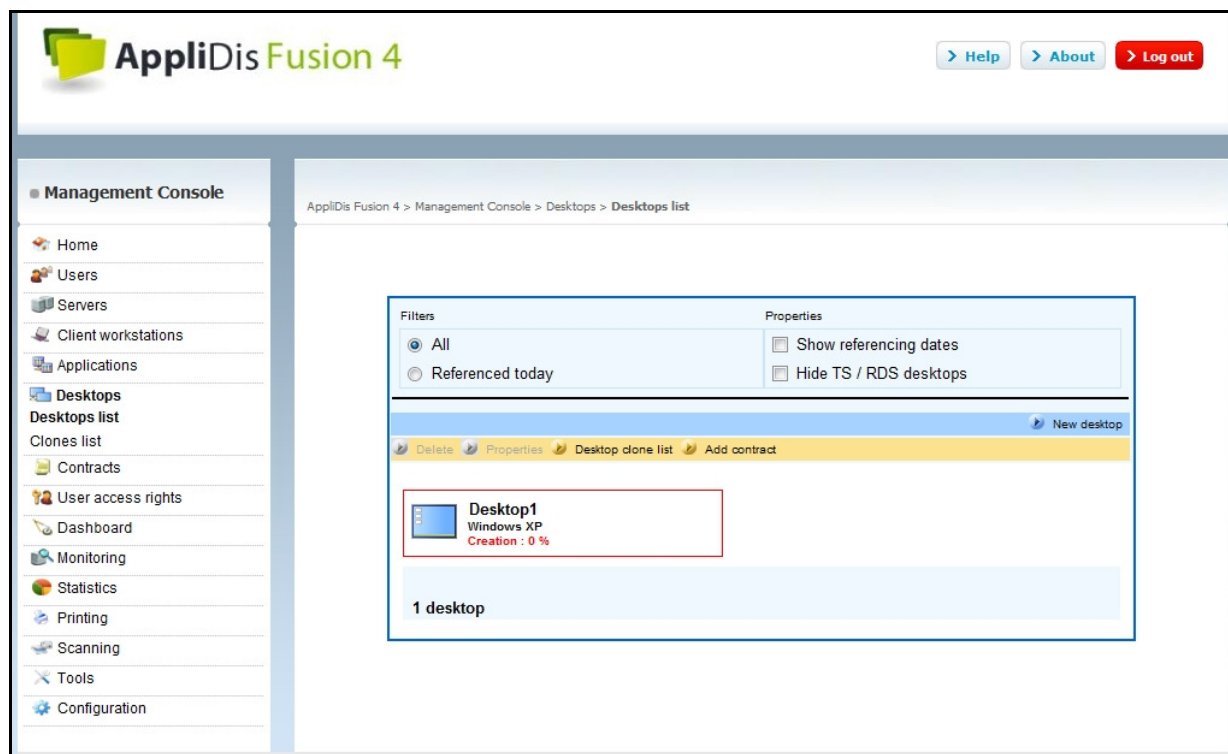


Figure 127 - Desktop installation process (AppliDis Management Console)

After validation, you can go back to the desktops' management interface. A new desktop has been added to the Desktop list. After a few seconds **"Creation"** is displayed in red indicating the percent completed for that installation.

When it reaches 100%, the desktop creation process is now complete. The list of created desktops now appears on the **Desktops → Clones list** page.

The screenshot shows the AppliDis Fusion 4 Management Console. The sidebar on the left contains the following menu items: Home, Users, Servers, Client workstations, Applications, Desktops (expanded), Desktops list, Clones list (selected), Contracts, User access rights, Dashboard, Monitoring, Statistics, Printing, Scanning, Tools, and Configuration. The main content area displays the 'Clones list' for 'Desktop1'. At the top, there is a dropdown menu set to 'Desktop1' and a 'New clone' button. Below this is a search bar with the text '[Tous | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | _ |]'. A table lists the clones:

Name	Desktop	System	IP Address	User	Permanent	In use	State
Desktop1_1_1	Desktop1	Windows XP	192.168.20.105		☐		Closed
Desktop1_1_2	Desktop1	Windows XP	192.168.20.106		☐		Closed
Desktop1_1_3	Desktop1	Windows XP			☐		Closed

Below the table, it says '3 clones' and there is a 'Refresh' button.

Figure 128 - Clones list Menu (AppliDis Management Console)

7.10 User group configuration

Go to the **Users menu → User groups** and click on the **Add groups** button.



Figure 129 - User groups menu (AppliDis Management Console)

Select **Domain user groups to import** into AppliDis. Then, click on the **OK** button.

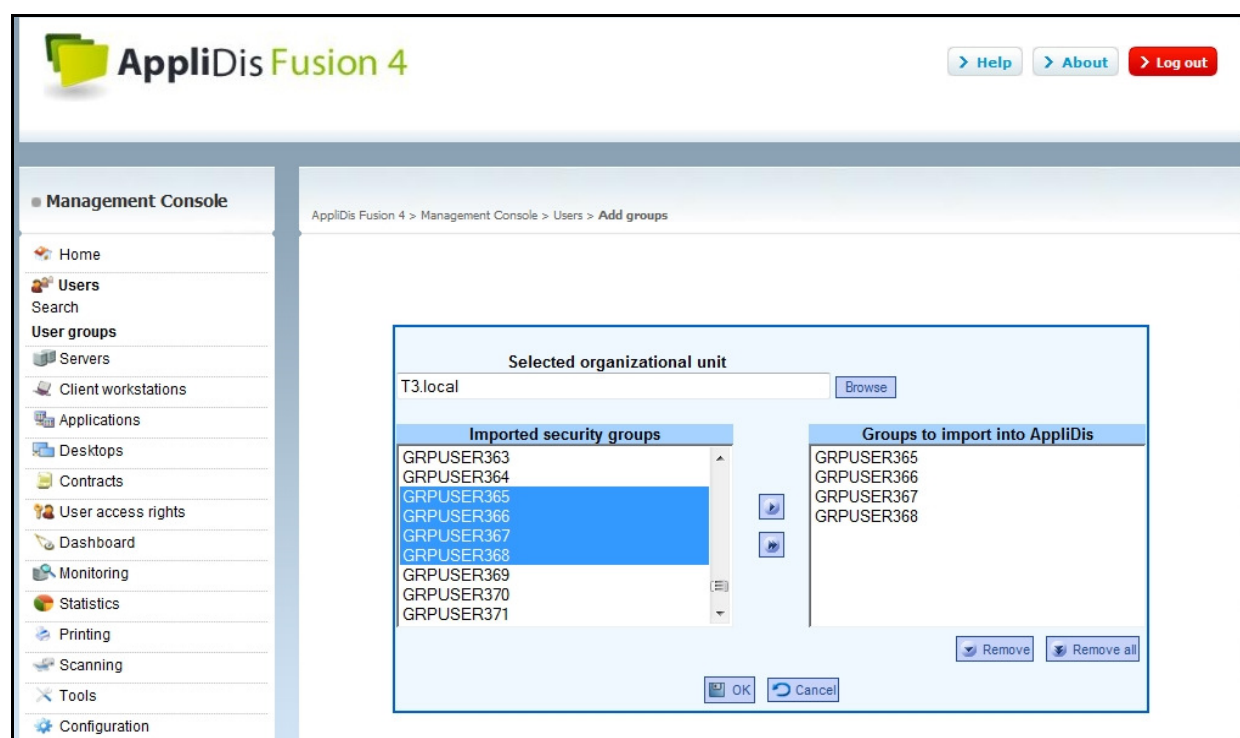


Figure 130 - Add groups by selected OU (AppliDis Management Console)

When the import process is complete, the list of imported groups appears on the **User → groups** page of the User groups menu option.



Figure 131 - User groups (AppliDis Management Console)

Please select a group you would like to give permanent access rights to the desktops and then click on the **Properties** button on the yellow bar.

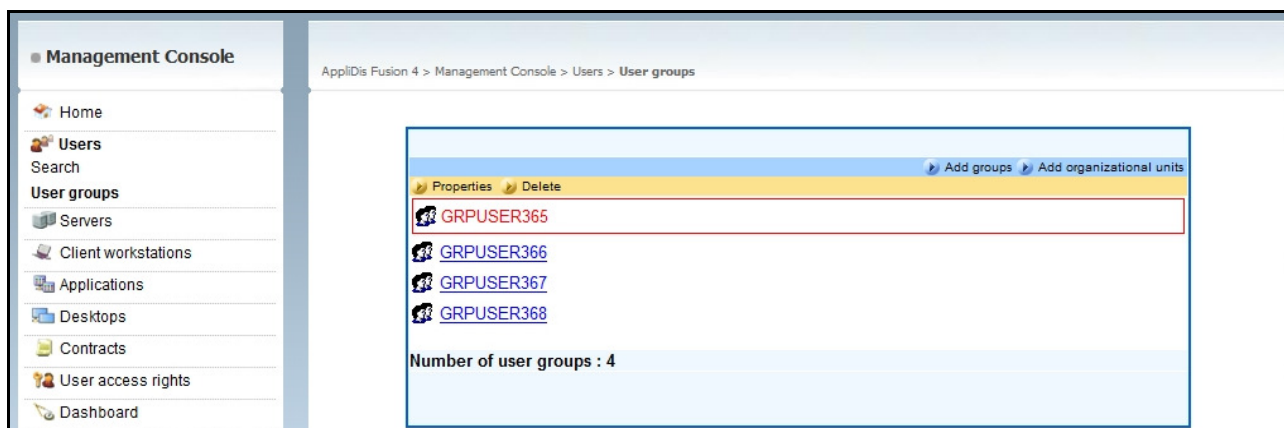


Figure 132 - User group properties (AppliDis Management Console)

And then, go to **Options**.

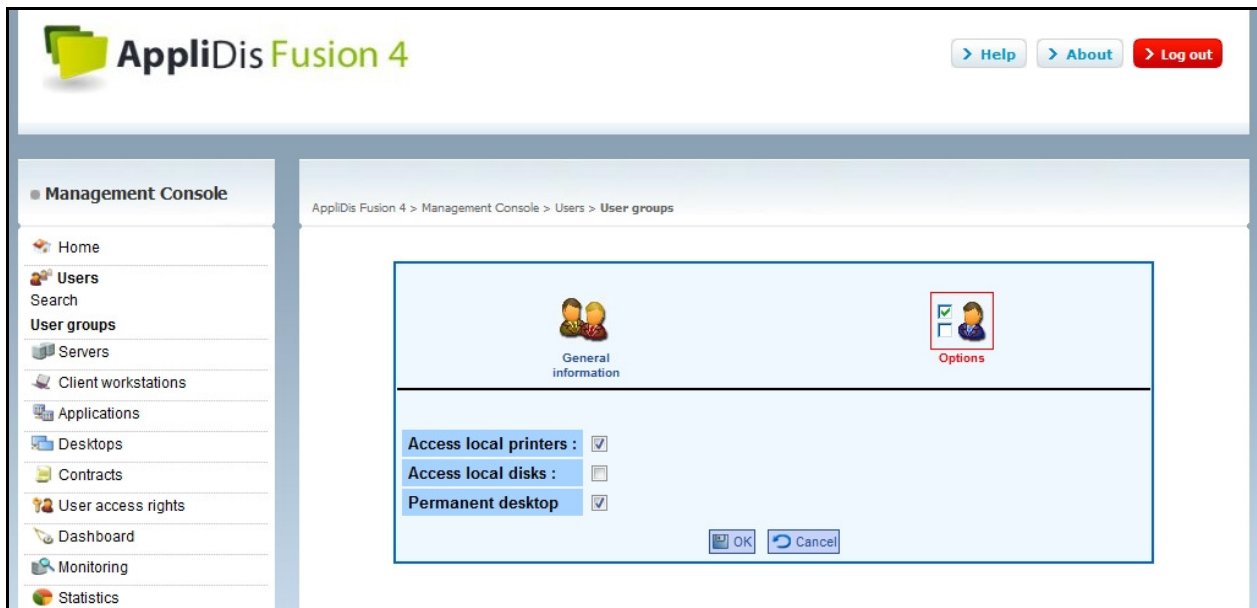


Figure 133 - Options from the User groups menu (AppliDis Management Console)

If the users from this group requires permanent access rights to the desktops: please tick the **Permanent desktop** checkbox and then click on the **OK** button.

7.11 Contract configuration

Go to the **Contracts** menu and then click on the **New contract** button (it is located on the right side of the window within the red square).

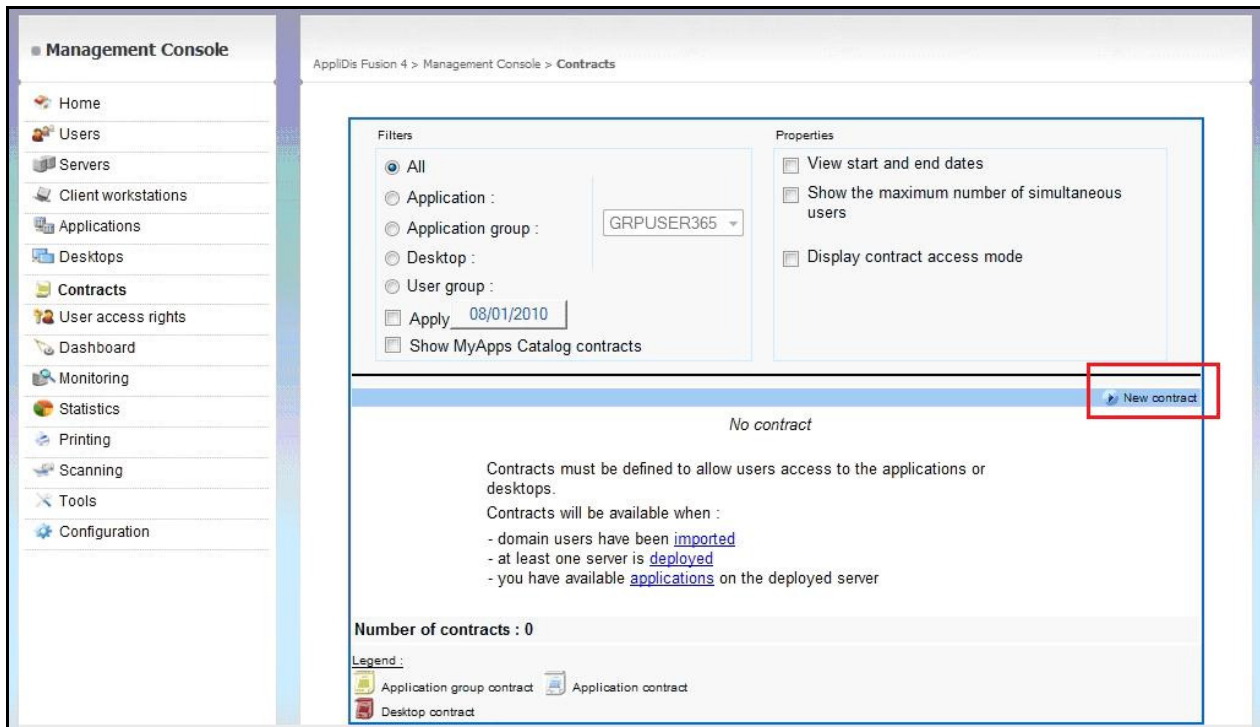


Figure 134 - New Contract (AppliDis Management Console)

The options are similar to the distribution of the applications, and allow AppliDis VDI to associate a user group to a desktop pool.

The screenshot shows the AppliDis Fusion 4 Management Console interface. On the left is a sidebar menu with options: Home, Users, Servers, Client workstations, Applications, Desktops, Contracts, User access rights, Dashboard, Monitoring, Statistics, Printing, Scanning, and Tools. The main area displays the 'New contract' form. The form includes the following fields and options:

- Type of contract :** Three radio buttons: ☐ for an application group, ☐ for an application, and ☒ on a desktop.
- Desktop :** A dropdown menu showing 'Desktop1'.
- User group :** A dropdown menu showing 'GRPUSER365'.
- Access mode :** A text field containing 'Every modes'.
- Contract beginning date :** A date picker showing '08/01/2010'.
- End of contract date :** A date picker followed by 'or' and a checked checkbox for 'Unlimited'.
- Maximum number of simultaneous users :** A text field containing '3'.

Below the form, a note states: 'Contract starts at 00 AM on the start date of the contract, and ends at 11:59 PM at the end of the contract date'. At the bottom right of the form are 'OK' and 'Cancel' buttons.

Figure 135 - Associate a user group to a Desktop (AppliDis Management Console)

Enter:

1. From the **Type of contract** field: please select **on a desktop**,
2. From the **Desktop** field: select the pool of desktops you want to associate, for example, 'Desktop 1'.
3. From the **User group** field: please select the group you want to associate, for example, 'GRPUSER365'.
4. Specify the start & end dates of the Contract.
5. Specify the maximum number of simultaneous users allowed to use the desktops for this contract. **Note:** the number **cannot** be higher than the actual pool size (defined in Localization, figure 11 where the pool size is set to 3).

And then, click on the **OK** button.

7.12 Client portal

Log on to the AppliDis client portal and go to **Your desktops** in the menu.

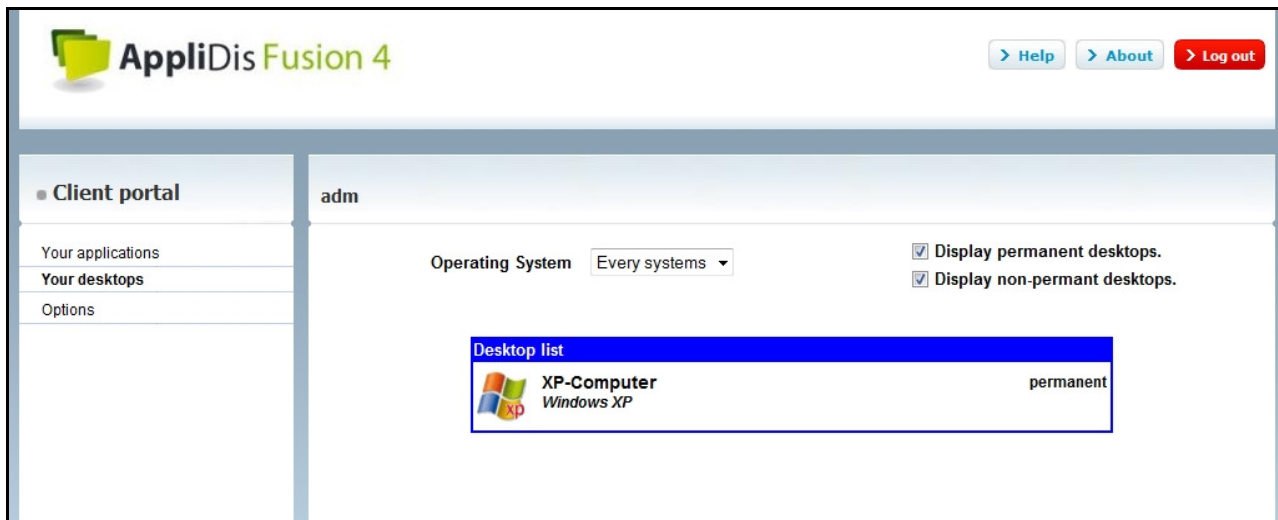


Figure 136 - Your desktops client portal menu (AppliDis client)

A list of desktops assigned to your group now appears. Click on a desktop to open, and connect to it.



Terminal Server services

Microsoft Terminal Server is essential for the use of AppliDis. This chapter provides an overview of this component which is present in the server versions of Windows and also provides information on aspects related to printing through the Terminal Server services.

1 Overview of the Microsoft Terminal Server

Microsoft Terminal Server is the application which makes the Windows operating system a multi-user system for the NT Server, 2000 Server, 2003 Server and 2008 Server versions. The first version to go on sale was Windows NT Server 4.0, Terminal Server Edition from July 1998. This version was a separate version for the operating system only, with the result that updates (patches and hot fixes) were managed separately from updates of Windows NT 4.0.

Subsequent versions - Windows 2000 Server, Windows 2003 Server and Windows 2008 Server - incorporate the Terminal Server services in a transparent way.

Each user who opens a session on a Terminal Server connection has his own environment with his own resources and is partitioned off from other sessions. The protocol used to transmit the video stream and user interactions (mouse, keyboard) is RDP (Remote Desktop Protocol). This protocol can be accessed from the following operating systems:

- Windows 2000/XP/Vista
- Windows NT (3.51 and 4.0)
- Windows 95/98
- Windows for Workgroups 3.11
- Windows CE
- Mac OS X
- Unix/Linux

2 Microsoft Terminal Server user licenses

2.1 Introduction

The AppliDis product does not handle Terminal Server licenses; these must be acquired from Microsoft or your usual retailer. You will have to activate the Application server(s) and parameterize the licenses.

2.2 License operating process

The general principle for Terminal Server licenses is that each hardware device accessing the Terminal Server services must have a license, which can be for a Windows 2000 server:

- Windows 2000 CAL (Client Access License)
- Windows 2000 professional license
- Windows XP professional license
- Terminal Server CAL

This means that if you have client workstations using Windows 2000 or XP Professional, you do not need to acquire special licenses to access Server 2000. Conversely, for all other operating systems on the client workstation, you will need to acquire Terminal Server CALs.

If at least one of your Application servers operates in 2003 Server environment, you must acquire 2003 Server CALs for all your client workstations (the same applies to 2008 Server).

Note: if you only have Service Pack 2 (SP2) on your 2000 servers, there is a hot fix to correct a problem of reassigning Terminal Server licenses. For more information on this problem and the associated corrections, please refer to Microsoft notice Q287687.

2.3 Installation and configuration

Installation is carried out in three stages:

- Installation of a Terminal Server license manager.
- Activation of the server(s) with Microsoft.
- Registration of the purchased licenses.

Installation of a Microsoft Terminal Server license manager

A license manager is required to manage the licenses of your network of Application servers. If you have several domains, you can choose to install several license managers, otherwise one manager is sufficient.

Note: in a configuration with Windows 2000 domain servers, the license manager must be activated on the domain controller.

1. In the Start menu, click on Settings (under Windows 2000 server), then on Control panel.
2. Select Add/Remove Programs, then Add/Remove Windows Components.
3. Check the Terminal Server services license manager box (for Windows 2000 Server) or the Terminal Server license management box (for Windows 2003 Server), then click on Next.
4. For Windows 2003 Server, select either a license server for the whole company or for the domain only.

Activating a Microsoft Terminal Server license server

This step is essential for the licenses to function on your Terminal Server servers. The following procedure is for direct activation via Internet, but it is also possible to activate the license servers by telephone or fax or through the Microsoft website.

1. In the Start menu, click on Programs, then on Administration tools, and select the Terminal Server services license manager.
2. Select the Terminal Server license server from the list of registered servers, and Activate the server to start the activation wizard.
3. Click on Next on the homepage.
4. Select Internet as method of connection and click on Next. A Microsoft activation server is then required.
5. Select the program for which you acquired the licenses, then click on Next.
6. On the following pages, enter the required information, then click on Next. Microsoft will send you an e-mail containing the PIN code to activate your server.
7. On the End of current process screen, update the PIN code either now or later. Click on Next to continue.
8. Enter the PIN code sent by Microsoft in the activation PIN code field, then click on Next. Your license server will then be activated.

Installing Microsoft Terminal Server licenses

This last step enables you to insert licenses which will authorize you to use the Terminal Server services from client workstations. The following method describes installation and activation via Internet, but this is also possible by fax, telephone or the website.

1. In the Start menu, click on Programs, then on Administration tools, and select the Terminal Server services license manager.
2. Select the Terminal Server license server from the list of registered servers, and Install licenses to start the license installation wizard.
3. On the Information on the program and the client license screen, select the information for your license program, then click on Next.
4. The request will then be processed and Microsoft will install the set of encrypted client license keys on your license server.
5. Click on Finish. Your server will then be correctly parameterized.

2.4 Microsoft Internet Connector license

This special license enables you to have up to 200 anonymous users connected to a Terminal Server Server. Microsoft specifies that the users accessing a Terminal Server server with this license should not be employees.

3 Printing with Terminal Server

3.1 Redirecting local printers

The redirection principle makes it possible to automatically direct the local printers of user workstations, in most cases without having to carry out configuration operations. The user's local printer will then be displayed in the form "Printer driver name / Client workstation name / Session number". This will then be the user's default printer.

The local printer must be configured and installed on a local printer port (LPT1 for example). Under Windows 2003, network printers are also redirected, while only the physical printers will be visible under 2000.

If you wish to deactivate the redirection of local printing, you must deactivate the option in the AppliDis administration console. To do this, you have to go to the "Access privileges" menu, then the "User group privileges / Options" sub-menu, and remove all the "Access to local printers" groups.

Note: if you encounter printing problems for files located on a shared network letter with a configuration having a Windows server 2000 SP3, the SP4 on the server must be updated or the hot fix must be requested from Microsoft (Q328020 "Redirected Printing Through a Terminal Services Session May Not Work").

3.2 Redirecting network printers

The redirection of network printers is automatic from RDP 5.1, and is organized in the same way as the redirection of local printers. The only difference that you will note is that in the case of a network printer, the redirection is of the type "___Printing server name_Printer driver name / Client workstation name / Session number".

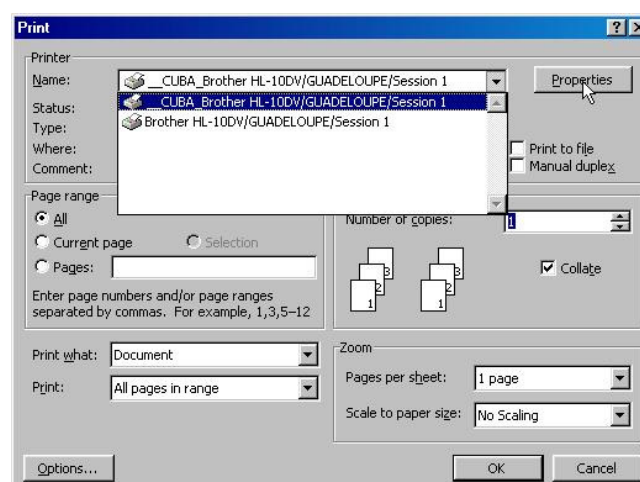


Figure 137 - Example of access to a printer in two modes (network and local)

3.3 Printers not recognized by the server

If printing does not function according to the aforesaid configurations, this may mean that your printer is not supported by default on the Windows 2000, 2003 or 2008 Application Server(s). Following a connection attempt, you will find messages of the following type in your server's events log: "The HP OfficeJet G Series Printer driver required for printer __NOIRMOUTIER_HP OfficeJet G Series is unknown. Contact the administrator to install the driver before reconnecting. ".

Checking a printer not recognized problem

1. In the control panel on the server, open the administration tools file, then select the Events observer.
2. In the System log section, search for events of the TermServDevices type
3. Click on the event to get the description of the problem and the confirmation of a printer conflict.

You can install the printer driver on the server at this point, but it is not recommended, since printer driver conflicts are the most frequent cause of sudden stops of the Terminal Server services.

The other possibility is to publish a configuration file containing the list of printers and to update it with the driver which is causing the problem. This file is used particularly when you add a printer driver and the system requires you to select the driver you wish to install from a preset list. The site is \WINNT\INF\NTPRINTF.INF (before making any modifications, it is advisable to make a backup of this file).

Adding a non-recognized printer

1. In the control panel on the client workstation, open the printers file
2. The name of the driver will be indicated in the Advanced or Details tab (depending on the client's operating system). Note this name carefully (same case must be used).
3. Open the file \WINNT\inf\NTprint.inf.
4. Search the "Previous Name" section.
5. Add a line to this section according to the following principle:
"Exact Name of the printer driver on the server" = "exact Name of the driver noted on the client workstation".

Caution: Driver names are case-sensitive in Windows

When modifying this file, the names of the drivers must be written in the correct case.

Here is an example of a line:

```
"Epson Stylus COLOR 740 ESC/P 2" = "EPSON Stylus COLOR 740"
```

3.4 AppliDis tools for printing

In the AppliDis Administration Server installation directory, you will find two executables located by default in the file: **c:\Program Files\Systancia\AppliDis\Tools:**

- **Printer manager:** GestDisPrinter.exe
- **Print queue manager:** GestDisSpooler.exe

These two utility companions can be copied on your servers and published for the users:

3.4.1 Printer manager

This utility allows the AppliDis user to access the Windows print management module located on the server. The user will be able to connect printers directly in his profile via AppliDis.

Caution: this utility will simply reference the changes in the current profile on the server. If you have several AppliDis servers, the user has to close all his AppliDis sessions so that the modifications carried out in the tool execution session are saved in this user's profile.

3.4.2 Print queue manager

This utility allows the user to access the Windows print queue manager from the AppliDis Server. If the user's workstation has a version that is equal to or higher than Windows NT4, this utility will also allow management of the local print queue. If the user is connected on AppliDis with an account that is separate from the local account, the queue will also be visible. Management will however be limited by the AppliDis user's Windows privileges on the local printer.

Index

A

Activating a server · 132
 Active Directory · 62, 66, 72
 Administration
 Access roles · 177
 Delegated administration · 176
 Zones · 177
 Administration roles · 177
 Administration Server redundancy
 Configuration with load balancing · 51
 Advance referencing · 100
 Alerts
 Configuration · 137
 Monitoring · 134
 Server not available · 138
 Application · 98
 Activate · 106
 Adding a new application · 102
 Adding an application registered on a server · 106
 Advance referencing · 100
 Advanced properties · 104
 Application · 112
 Application distribution statistics for servers · 159
 Applications in use · 129
 Checking application privileges · 128
 Checking option privileges · 128
 Checking the automatic recording of an application · 101
 Icon · 113
 Installation · 98
 Listing of applications available on a server · 91
 Location · 105, 106, 107
 Manual referencing · 102
 Maximum number of runs · 15
 Normal · 112
 Priorities · 110
 Priority · 105
 Referencing · 98
 Renaming an application · 101
 Resolution · 104
 Responsiveness · 104
 Servers available to an application · 102
 Statistical summary · 157

 Statistics · 160
 Usage distribution statistics · 161
 Usage statistics · 160
 AppliDis
 Client in desktop mode · 20
 Client, application portal · 18
 Client, AppliDis Launcher · 22
 Client, thin client mode · 21
 Evaluation Version · 15
 AppliDis group · 71
 Authentication · 48

C

Connection · 65
 Contract · 64, 109, 123, 124, 125, 126
 Adding a contract for an application · 124
 Adding a contract for an application group · 125
 Modification · 126
 Modifying a contract · 126
 Principle · 123
 Removing · 125
 Removing a contract · 125
 CPU
 Usage · 129

D

Dashboard · 129
Databases
 Backup databases · 190
 Directory · 54
 Microsoft SQL 2005 Express · 56
 Microsoft SQL Server · 55, 57
 Microsoft SQL Server 2000 · 190
 Requirements · 34
 Secondary databases · 190
 SQL 2005 Express · 191
 SQL Server 2000 · 34
 SQL Server 2005 · 30, 31, 32, 33, 34, 35
Delegated administration
 Contracts · 178
 Delegated administration · 176
 Applications · 178
 Roles · 177

Servers · 178

Users · 177

Delegated administration

Statistics · 178

Delegated administration

Monitoring · 178

Delegated administration

Configuration · 178

Delegated administration

Groups · 178

Delegated administration

OU's · 178

Desktop

Statistics · 165

Usage distribution statistics · 167

Usage statistics · 166

directory · 70, 71, 72

Directory · 63, 66, 71, 78

Dynamic · 72, 184

synchronized · 66, 184

Domain controller · 47

Dynamic · 72

H

High availability

AppliDis database · 24

IP Aliasing · 24

Virtual IP · 24

High Availability

Administration · 24

Applications · 23, 24

Gateway · 25

Installation · 53

Redundancy · 23, 24, 34, 51, 53, 83

I

Icon · 113

Installation

Installation of the AppliDis Server · 63, 84

Internet Information Server · 36, 37

Terminal Server services · 39, 41, 42, 44

Uninstalling AppliDis · 60

Uninstalling the AppliDis Server · 90

IP address

Modification in AppliDis · 86, 87

IP Address

requirements · 46

L

Languages · 192

License · 15, 39, 180, 245

Activating a Terminal Server license server · 246

AppliDis Licenses · 15, 180

Installation of a Terminal Server license manager · 245

Installing Terminal Server licenses · 246

Terminal Server Internet Connector License · 247

Terminal Server user licenses · 245

Local drives · 79

M

Monitoring

Alarm settings · 137

Alerts · 134

CPU · 138

Databases · 138

Disks · 138

Events logs · 134

Memory · 138

Monitoring authority · 139

Resources · 136

Transmission methods · 140

TSE sessions · 137, 138

N

Novell · 66

O

OpenLDAP · 66

Options · 184

Automatic connection · 185

Dynamic management of directories · 184

Pass-Through · 185

Priority · 184

P**Print**

- Access to local printers in AppliDis** · 80
- AppliDis tools for printing · 248
- Print queue manager · 249
- Printer manager · 249
- Redirecting local printers · 247
- Redirecting network printers · 247
- Printing · 80, 247
- Privileges · 18, 81, 90, 126
 - Access to servers** · 127
 - Applications · 128
 - Checking application privileges** · 128
 - Checking option privileges** · 128
 - options · 128
 - servers · 127

R

- RDP · 87, 244, 247
- Recovery after an incident** · 195
- Redundancy
 - Secondary databases · 190
- Router · 52, 86, 87

S

- Scripts · 192
- Secondary databases
 - Redundancy · 190
- Serial number · 15, 180
- Server · 81
 - Activating** · 132
 - Applications available on a server** · 91
 - Basic configuration with a server · 48
 - Configuration with a router · 52
 - Configuration with load balancing · 50
 - CPU usage · 129
 - Deactivating** · 131
 - Deactivation** · 131
 - General information** · 85
 - Installation** · 84
 - Instantaneous information** · 129
 - Maximum number of servers · 15
 - Memory and CPU usage statistics** · 158

- Modification of the connection port for the Gateway Server · 87
- Modification of the IP address** · 86, 105
- Referencing** · 81
- Requirements · 28
- Server Group** · 90
- Setting the IP address for configuration with router** · 87
- Statistical summary** · 157
- Statistics · 157
- Uninstalling · 90
- Usage distribution statistics · 159, 164
- Usage statistics** · 158
- User distribution statistics** · 159
- Virtual IP Address · 14, 24, 85
- Sessions** · 129
- Synchronize · 72

T

- Taking control** · 132
- Terminal Server · 39, 248
 - Installing the Terminal Server services** · 39, 41, 42, 44
 - Requirements · 34
- Thin clients
 - Configuration · 26, 27
- Thin Clients
 - Load balancing · 83

U

- Uninstalling** · 60
- User · 66
 - Limited number of simultaneous users · 15
- Statistical summary** · 157
- Statistics · 163
- synchronization · 66
- Usage statistics** · 163
- User distribution statistics for servers** · 159
- User group**
 - Add groups · 77
 - Remove · 79
- Synchronize a group** · 72
- synchronize all groups** · 72
- User Groups**

Add Organizational Units · 77, 78

Users

Dynamic management · 63

Static management · 63

V

Virtual IP · 14, 24, 26, 85

Z

Zones · 177